CAPÍTULO QUINTO

PELIGROS TECNOLÓGICOS

María José Caro Bejarano

RESUMEN

La Estrategia Española de Seguridad menciona los peligros tecnológicos como uno de los potenciadores del riesgo, que podrían materializarse debido a un uso malintencionado o incorrecto de las incesantes innovaciones que se producen en terrenos tales como las tecnologías de la información y la comunicación, la industria armamentística o en campos de investigación tecnocientífica, como la biotecnología, la nanotecnología, la genética o la inteligencia artificial, entre otros.

El avance de las tecnologías en unos casos ha acortado las distancias, el tiempo y las diferencias de desarrollo entre los ciudadanos, entre los Estados y los actores no estatales, sin embargo, en otros casos se ha dado lo contrario, y las diferencias se incrementan y definen con posiciones más extremas.

Mientras en el pasado se necesitaban importantes recursos materiales y humanos para ejercer una influencia política o económica a escala global, las fronteras se han hecho permeables conforme el poder se traslada del mundo físico al mundo virtual. Se necesita un espacio digital seguro para garantizar la estabilidad en la economía mundial y el equilibrio de poder.

El ciberespacioy las redes de información y comunicación soportan la prestación y gestión de muchas infraestructuras y servicios, privados y de las administraciones públicas. Su seguridad puede verse comprometida por causas técnicas, fenómenos naturales o por ataques ilícitos. Los posibles agresores son variados –terroristas, crimen organizado, empresas, estados o individuos aislados–.

El ciberespacioes asimismo un ámbito para el espionaje por parte de agentes criminales y de otros estados para la obtención de información y de datos personales. Además del coste económico genera una pérdida de confianza entre los ciudadanos sobre las medidas de seguridad de este ámbito.

La potencialidad de estos peligros tecnológicos se encaran desde la Estrategia con un enfoque preventivo e integral y fomentando la protección y la capacidad de resistencia y recuperación ante una vulnerabilidad.

Palabras clave

Peligros tecnológicos, tecnologías de la información y la comunicación, biotecnología, nanotecnología, genética, inteligencia artificial.

María José Caro Bejarano

ABSTRACT

The Spanish Security Strategy mentions technological hazards as one of the risk multipliers, which could be realized due to malicious or misuse of the incessant innovations that occur in areas such as information and communication technologies, arms industry or techno-scientific research fields such as biotechnology, nanotechnology, genetics and artificial intelligence among others.

The technologies advance has shortened distances, time and the differences in development among citizens, states and non-state actors. However, the opposite has occurred in other cases and the differences are increasing and defining with more extreme positions.

Whereas significant human and material resources were required in the past to exert political or economic influence on a global scale, the boundaries have become permeable as the power shifts from the physical world to virtual one. A secure digital space is required to ensure stability in the world economy and balance of power.

Cyberspace and information and communication networks support the delivery and management of many infrastructure and services of private and public administrations. Their security may be compromised due to technical reasons, natural phenomena or unlawful attacks. Potential attackers are varied-terrorists, organized crime, companies, States or single individuals

Cyberspace is also an area for espionage agents by criminals and other States, to obtain information and personal data. In addition to the economic cost, it raises a loss of confidence among citizens about the security of this area.

The strategy faces the technological hazards potential with a preventive and comprehensive approach and promoting protection and resilience from a vulnerability.

Key words

Technological hazards, information and communication technologies, biotechnology, nanotechnology, genetics, artificial intelligence.

INTRODUCCIÓN

Significativa presencia de la tecnología en la EES

La Estrategia Española de Seguridad (EES)[1] aborda en su capítulo 3 cinco factores considerados como potenciadores de riesgo que «propician la propagación o transformación de las amenazas y riesgos e incrementan nuestra vulnerabilidad». Estos factores transnacionales son: «Las disfunciones de la globalización, los desequilibrios demográficos, la pobreza y la desigualdad, el cambio climático, los peligros tecnológicos, y las ideologías radicales y no democráticas.»

De ellos, los peligros tecnológicos están directamente relacionados con la tecnología, aunque esta también se menciona en la Estrategia como un vehículo en el que se apoyan otros potenciadores de riesgo. Además, en el capítulo 4, sobre amenazas, riesgos y respuestas, la tecnología aparece como parte del problema y de la solución.

Por una parte, entre los seis potenciadores de riesgo, la tecnología aparece en «Las disfunciones de la globalización» cuando se afirma que «La 'tecnología' y las comunicaciones han mejorado la calidad de nuestras vidas y han puesto el mundo a nuestro alcance. Nuestras empresas exportan a los cinco continentes. Se ha abierto la puerta a mecanismos de gobernanza global que abordan problemas que nos afectan directamente». Como contrapeso a este argumento se aclara que «Asimismo, para poder gestionar sistemas económicos, institucionales y 'tecnológicos' más interconectados –y, por tanto, más eficientes pero también más complejos y vulnerables– es necesario construir sistemas más flexibles, resistentes y con capacidad de recuperación»[2].

En «Los peligros tecnológicos», se destacan algunos aspectos positivos y negativos de la misma: «La 'tecnología' es una creciente fuente de progreso. Internet y los teléfonos móviles forman ya parte de nuestra vida cotidiana, nos abren al mundo y generan riqueza, pero nos hacen también más vulnerables. La 'tecnología' puede potenciar o crear nuevas amenazas y riesgos para la seguridad.

Con la 'tecnología' de hoy es imaginable que un grupo terrorista o un país enemigo colapsara el tráfico en el 'ciberespacio', paralizando, por ejemplo,

[1] La Estrategia Española de Seguridad fue aprobada el 24 de junio de 2011. Véase www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/EstrategiaEspanolaSeguridad_junio2011.pdf.

[2] La EES menciona varias veces «la capacidad de resistencia y recuperación» aplicada a sistemas e instrumentos. Este concepto está tomado del término «resiliencia» que aplicado al campo de la psicología es la capacidad humana de asumir con flexibilidad situaciones límite y sobreponerse a ellas; y al campo de la mecánica es la capacidad de un material elástico para absorber y almacenar energía de deformación (diccionario de la RAE). La traducción anglosajona es el término resilience.

el sistema financiero y parte de los servicios públicos. Por eso, la 'ciberseguridad', relacionada con las infraestructuras vitales para el funcionamiento de un país, se ha convertido en un ámbito clave para la seguridad de cualquier estado».

Menciona algunas ramas novedosas de la tecnología: «Los avances en 'biotecnología', 'nanotecnología', genética o inteligencia artificial, abren mundos de posibilidades incalculables que suponen grandes progresos para la humanidad. Pero también conllevan riesgos e incluso dilemas éticos aún por identificar».

Y resalta el carácter dual militar/civil de la tecnología: «Si durante años la innovación 'tecnológica' militar fue pionera y dio lugar a aplicaciones civiles de gran valor, los descubrimientos e inventos civiles van hoy por delante en bastantes ocasiones. Es necesaria una relación estratégica entre ambos sectores en beneficio de la seguridad en general. Quedarse por detrás de nuestros competidores en capacidad de innovación tendría un serio impacto en nuestra competitividad y desarrollo, y, por tanto, en nuestra seguridad».

En «Las ideologías radicales y no democráticas» se aclara que «este radicalismo se ve espoleado por la composición demográfica y la facilidad para propagarlo con las nuevas 'tecnologías' de la información», es decir, actuaría como correa de transmisión de un fenómeno sociológico.

Por otra parte, entre las amenazas y riesgos del capítulo 4 también está presente la tecnología.

En la amenaza de los «conflictos armados», al abordar las líneas estratégicas de acción y mencionar a las Fuerzas Armadas y sus capacidades, se hace referencia a que estas han de «ser 'tecnológicamente avanzadas' –como exigen la eficacia y las características de las tareas que se les encomiendan–». Dentro de las mismas líneas estratégicas de acción también se incluye la base industrial y 'tecnológica' de la defensa y seguridad que «constituye un elemento esencial de nuestra capacidad de respuesta a las amenazas y riesgos. […] La aplicación efectiva de las directrices de seguridad requiere de la adecuada organización de capacidades industriales y 'tecnológicas' y de la movilización de los recursos financieros y materiales necesarios».

«La concepción integral y transversal de una seguridad, responsabilidad de todos, implica incluir en su definición estratégica a los responsables institucionales de la política industrial en general, a los agentes industriales y a los centros universitarios y de investigación científico-'tecnológica'».

«El funcionamiento de esta base industrial y 'tecnológica' asociada a la seguridad integral no limita sus efectos a la provisión de sistemas, bienes y equipa-

mientos para los responsables de la seguridad. Muchos de los desarrollos e innovaciones 'tecnológicas' que nacen con esta finalidad encuentran aplicaciones adicionales y duales que extienden sus beneficios a la totalidad de la sociedad».

Al plantear la amenaza del «terrorismo», la estrategia señala que «Las organizaciones terroristas internacionales […] aprovechan ciertas características de la nueva sociedad global, como el desarrollo 'tecnológico' […] para reclutar miembros, obtener recursos...». De nuevo, la tecnología puede usarse como instrumento de otras amenazas.

El «crimen organizado» se presenta como «una de las más graves amenazas para la seguridad del Estado y de sus ciudadanos. Sus distintas modalidades son un poderoso factor de desestabilización de los cimientos políticos y económicos de la sociedad española y europea». Entre estas amenazas la EES destaca entre otras «los 'delitos tecnológicos'»[3] y propone como una de las líneas estratégicas de acción «Incrementar [entre otros] los recursos 'tecnológicos' de las unidades especializadas contra el crimen organizado».

La inclusión de la amenaza «inseguridad económica y financiera» es una novedad en esta primera estrategia de seguridad, en ella destaca el papel fundamental del sector privado en la seguridad, «muchas de cuyas empresas son propietarias o gestoras de servicios e infraestructuras relacionados con la seguridad». «Este sector privado puede aportar importantes capacidades», entre ellos se incluye «su saber hacer 'tecnológico'».

Al tratar la amenaza de la «vulnerabilidad energética», la EES mencionadentro de las líneas y redes de abastecimiento las «'infraestructuras' energéticas 'críticas': el sistema gasista, el sistema de transporte y distribución de petróleo

[3] El 23 de noviembre del 2001 el Consejo de Europa aprobó el Convenio de Budapest sobre la lucha contra el delito cibernético. Hoy en día, ese tratado representa solo las directrices internacionales aceptadas sobre cómo proteger la libertad, la seguridad y los derechos humanos en la red. Más de ciento veinte países están cooperando con el Consejo de Europa para reforzar su legislación y la capacidad para hacer frente a los delitos informáticos, muchos de ellos como parte de la Convención sobre el Cibercrimen, que ha sido ratificada por treinte y tres países y firmado por otros catorce. Ocho países han sido recientemente invitados a participar. Esta Convención ha tenido un impacto mundial y ha dado lugar a una legislación del delito cibernético más fuerte y más armonizada en todo el mundo, la cooperación internacional más eficaz en la investigación y el enjuiciamiento de los delitos basados en Internet y el estrechamiento de las asociaciones público-privadas. El cibercrimen o ciberdelito, entre los que se contemplan la intrusión ilegal en los ordenadores, la interceptación de comunicaciones privadas, ataques de denegación de servicio, robo de identidad y el fraude, o la explotación sexual de los niños, afecta a los derechos de las personas de todo el mundo. Como la tecnología avanza mucho más rápido que las respuestas jurídicas, hay una necesidad de hacer frente constantemente a nuevos retos, a menudo relacionados con la protección de datos, como el acceso transfronterizo a los datos de aplicación de la ley y el intercambio de información entre los sectores público y privado. La legislación insuficiente o incompatible en muchos países sigue siendo un obstáculo importante para un enjuiciamiento exitoso internacional de los delincuentes.

y el sistema eléctrico, fundamentalmente las grandes infraestructuras de la red de transporte y generación»que «son identificadas comoactivos estratégicos para la seguridad por el Plan de Protección de Infraestructuras Críticas, pues su funcionamiento es indispensable y no permite soluciones alternativas. Es esencial, por tanto, garantizar su seguridad, dotándolas de sistemas redundantes e independientes de otras 'tecnologías' y operadores».

Las «ciberamenazas» están relacionadas directamente con las «tecnologías» de la información y las comunicaciones. Según narra la EES «Cada vez [más] una mayor parte de nuestra actividad se desarrolla en el 'ciberespacio', donde las amenazas pueden ocasionar graves daños e incluso podrían paralizar la actividad de un país. Los 'ciberataques' más comunes tienen fines comerciales, pero también estamos expuestos a agresiones por parte de grupos criminales, terroristas u otros, incluso de estados. Las nuevas 'tecnologías' de información y comunicación ofrecen nuevos y más sofisticados medios para el espionaje y la contrainteligencia».

La EES considera que «Hay factores legales y 'tecnológicos' que incrementan las posibilidades de que las 'ciberamenazas' se materialicen… 'Tecnológicamente', Internet fue creado para ser útil y sencillo, no para ser seguro. La creciente interconexión de la red, incluyendo necesariamente las infraestructuras, suministros y servicios críticos, incrementa los niveles de riesgos sobre estos».

«Es necesario seguir impulsando la toma de conciencia y la formación sobre los riesgos, reforzando las políticas específicas y los procedimientos de seguridad en los sistemas de información y comunicaciones de ciudadanos, empresas e instituciones, y reduciendo la dependencia de la 'tecnología' de seguridad de terceros países». Sobre esto incide una de las líneas estratégicas de acción.

Al plantear las ciberamenazas se expone que «el 'espionaje' se ha adaptado al nuevo escenario de seguridad, aprovechando las posibilidades que ofrecen las nuevas 'tecnologías' de la información y comunicación y el proceso de globalización. Las intromisiones en el 'ciberespacio' para obtener información son cada vez más comunes y preocupantes. De particular importancia es también el 'espionaje económico', consistente en la adquisición ilícita de información, patentes o 'tecnologías' críticas, e incluso en la influencia ilegal en decisiones políticas de carácter económico. Su impacto potencial es cada vez mayor por su capacidad de dañar el sistema económico y afectar al bienestar de los ciudadanos».

Respecto a la amenaza de «emergencias y catástrofes» la EES destaca que «A pesar de los avances 'tecnológicos' y sociales, los riesgos de origen natural siguen golpeando a la humanidad y produciendo catástrofes. […] Las catástrofes también pueden tener su origen en la actividad humana, como el desastre nuclear de Chernóbil. O pueden ser resultado de la combinación de ambos, como el *tsunami* en Japón y consiguiente accidente nuclear en la central de Fukushima…

Y, como país industrializado, también pueden afectarnos otros 'riesgos de naturaleza tecnológica'».

En este aspecto destaca el papel de la UME, cuya «principal misión es intervenir en emergencias que tienen su origen en riesgos naturales (terremotos, inundaciones, incendios forestales o inclemencias invernales, entre otros) o 'tecnológicos'».

En la amenaza a las «infraestructuras, suministros y servicios críticos» se plantea que «Fenómenos naturales extremos, atentados terroristas o 'ciberataques' […] pueden dañar las infraestructuras críticas, suministros y servicios críticos que sustentan nuestra vida y el desenvolvimiento de nuestra sociedad».

«Entre las infraestructuras, suministros y servicios críticos relevantes destacan la energía, las redes de comunicación y las finanzas –ya tratados en otros apartados–, el transporte, el agua, la salud o la alimentación».

En uno de los suministros críticos, elagua, la tecnologíaaparece relacionada con su seguridad**: «**La seguridad del abastecimiento pasa ahora por profundizar en su uso eficiente y sostenible, en las medidas de gestión de la demanda, en las 'tecnologías' de ahorro, especialmente en los regadíos agrícolas, y en la depuración y reutilización. España es hoy uno de los países líderes en 'tecnologías' del agua como depuración, potabilización o desalación».

Consideraciones sobre la tecnología

Bajo la denominación de peligros tecnológicos la EES agrupa diferentes tipos de tecnologías que pueden ser tratados de forma independiente. Así, menciona la tecnología relacionada con el ciberespacio, junto con otras disciplinas que combinan varias tecnologías como son la biotecnología, la nanotecnología, la genética o la inteligencia artificial. La consideración de peligros tecnológicos se podría ampliar para incluir otras tecnologías cuyo mal uso pudiera también provocar o potenciar cualquiera de las amenazas presentes en la Estrategia, como las tecnologías aplicables al desarrollo nuclear, químico, radiológico, identificación biométrica, etc.

Los avances tecnológicos son un factor de competitividad. Países como EE. UU., Japón o Corea del Sur apostaron en su día por el desarrollo tecnológico como motor de recuperación del país después de la participación en diversas guerras. Es una vía que permite a los investigadores y científicos, así como a las empresas y países, ser más competitivos.

La tecnología también puede actuar en el ámbito de la seguridad de forma positiva o negativa, disminuyendo o potenciando los riesgos. Puede ser poten-

ciador de estabilidad o potenciador de riesgos y amenazas, como todo avance presenta esta dualidad según el uso que el factor humano le confiere. Es responsabilidad de todos asegurarnos de que el uso que se le da a la tecnología es el más beneficioso para los intereses de un país y para la humanidad. En este capítulo se analizará su papel como potenciador de riesgo sin olvidar la importancia que ha tenido para el desarrollo de la humanidad.

La EES destaca el papel pionero e innovador de la tecnología militar al principio de su desarrollo, que, a su vez, produjo aplicaciones civiles de gran valor. Sin embargo, desde hace tiempo, es la tecnología civil la que adelanta a la militar. La EES defiende la necesidad de «una relación estratégica entre ambos sectores [civil y militar] en beneficio de la seguridad en general. Quedarse por detrás de nuestros competidores en capacidad de innovación tendría un serio impacto en nuestra competitividad y desarrollo, y, por tanto, en nuestra seguridad».

Mayor vulnerabilidad de la humanidad frente a la tecnología

Nos movemos en un mundo donde casi todos dependemos de los ordenadores, los teléfonos móviles y otros dispositivos electrónicos. Al mismo tiempo que el progreso tecnológico nos facilita la vida diaria, las transacciones comerciales, las comunicaciones, etc., este mismo progreso nos hace más dependientes de la tecnología y, por tanto, más vulnerables ante su uso.

La innovación, tanto científica como social, también afecta al conflicto mismo. Es probable que estados, así como actores no estatales, empleen medios asimétricos que son más baratos y menos atribuibles que los medios convencionales. Al mismo tiempo, algunos actores no estatales tienen significativa capacidad militar convencional, y algunos aspiran a desarrollar capacidades de armas biológicas y nucleares. En todo el mundo el carácter de los conflictos está cambiando.

Pero también somos vulnerables ante la naturaleza a la que pretendemos y creemos tener controlada. Por ejemplo, ante un huracán o una tormenta solar, las comunicaciones y las redes eléctricas pueden verse afectadas y con ello la seguridad.

Veamos este caso con mayor detalle. Las partículas procedentes de las erupciones solares pueden afectar al campo magnético terrestre, el cual dirige las partículas cargadas (electrones y protones) hacia los polos. Al penetrar en la atmósfera transmiten energía, cuyo exceso, en forma de una luz difusa y coloreada, se conoce como auroras boreales.

Nuestras redes eléctricas no están diseñadas para resistir esta clase de súbitas embestidas energéticas, que se producen con cierta regularidad. Desde

que somos capaces de realizar mediciones, la peor tormenta solar de todos los tiempos se produjo el 2 de septiembre de 1859. Conocido como «el evento Carrington», por el astrónomo británico que lo midió, causó el colapso de la mayoría de las redes mundiales de telégrafos. En aquella época, la energía eléctrica apenas empezaba a utilizarse, por lo que los efectos de la tormenta casi no afectaron a la vida de los ciudadanos. En 1972 una tormenta magnética provocó interrupciones en la red telefónica de Illinois (EE. UU.) mientras que en marzo de 1989, en Quebec, se colapsaron las redes de tendidos eléctricos y dejó a seis millones de personas sin electricidad y pérdidas por 50 millones de dólares. Durante 2012 se han registrado algunas llamaradas solares y tormentas electromagnéticas, según la agencia de meteorología espacial de EE. UU.[4]. La tormenta de enero alteró las comunicaciones por radio en Australia, China e India. Por eso, el conocimiento de la meteorología espacial, hoy que estamos tan «conectados», puede evitar daños millonarios a los sistemas eléctricos a nivel global.

Un informe publicado en 2009 por la Academia Nacional de Ciencias de Estados Unidos (NAS[5]), subrayaba la existencia de dos grandes problemas de fondo: el primero, y ya mencionado, es que las modernas redes eléctricas resultan especialmente vulnerables a esta clase de tormentas procedentes del Sol.

El segundo problema es la interdependencia de estas redes respecto de los sistemas básicos que garantizan nuestras vidas, como suministro de agua, tratamiento de aguas residuales, transporte de alimentos y mercancías, mercados financieros, red de telecomunicaciones, etc. Muchos aspectos cruciales de nuestra existencia dependen de que no falle el suministro de energía eléctrica[6].

Según la agencia estadounidense NOAA (National Oceanic and Atmospheric Administration[7]), igual que las redes de transmisión de energía y los satélites de comunicaciones, también las aerolíneas y las plataformas petrolíferas pueden verse afectadas. Así, existe el riesgo de que se produzcan interrupciones en el suministro eléctrico, en los sistemas de navegación por satélite y de comunicación por radio. Por ello, en esas ocasiones se desvían los vuelos comerciales que cubran rutas cercanas a los polos para garantizar la seguridad.

El caso de las tormentas solares ya se ha considerado, al menos, por parte de la OCDE[8] y la Estrategia de Seguridad Británica. Además, el Parlamento bri-

[4] Véase www.swpc.noaa.gov Space Weather Prediction Center.
[5] Se puede consultar en www.nasonline.org
[6] Sin estar relacionado con este tema solar, baste recordar que el fallo de suministro eléctrico tras el *tsunami* provocado por el terremoto de Japón el pasado marzo de 2011 afectó seriamente a los reactores nucleares de la central de Fukushima, y esto, a su vez, tuvo sus implicaciones en la modificación de los programas nucleares de otros países en el otro extremo del mundo, como Alemania.
[7] Véase www.noaa.gov
[8] Organización para la Cooperación y el Desarrollo Económico.

tánico publicó en febrero un informe que reconoce las tormentas solares como una amenaza para la seguridad nacional.

En concreto, el informe de la OCDE de julio 2011 *Future Global Shocks*[9] declaraba el riesgo de tormenta solar como uno de los «cinco grandes riesgos potenciales» que pueden llegar a desencadenarse sobre nuestra sociedad mundial en los próximos años, con efectos devastadores muy cuantiosos y difíciles de evaluar. Además de este gran riesgo potencial «de tormenta solar que pudiese producir un apagón eléctrico y tecnológico y perturbaciones en las comunicaciones por satélite», los otros cuatro tomados en consideración por la organización internacional serían: pandemias, ciberataques que afecten a infraestructuras, crisis financieras y revueltas socio económicas (junto con algunos eventos extremos). Junto a este informe general, la OCDE procedió a abordar este riesgo concreto de modo especializado en un segundo informe titulado *Geomagnetic storms*[10].

En este informe se formulan distintas recomendaciones a la comunidad internacional y a las autoridades estatales para el desarrollo de políticas públicas preventivas frente a la «potencial pérdida indirecta de vidas» por el fallo de los sistemas eléctricos y de energía; en especial, debido a las «consecuencias en cascada» asociadas a la posible larga duración de tal situación, una vez caídos los sistemas y hasta lograr su recuperación ciudad a ciudad.

Respecto a la Estrategia de Seguridad Británica, publicada en octubre de 2010, esta proporciona tres grupos de riesgos prioritarios según una metodología de clasificación que considera su probabilidad y su impacto.

El primer grupo de riesgos[11] se refiere a »un accidente importante o un suceso nacional que requiere una respuesta nacional». Una meteorología espacial inclemente forma parte de este primer grupo de riesgos emergentes debido a su potencial impacto sobre las infraestructuras del país.

En un informe publicado en febrero el Parlamento británico[12] admitía las tormentas solares como una amenaza para la seguridad nacional.

Este informe sugiere que en los próximos años puede suceder una alteración electromagnética, ya sea, por una tormenta solar como fenómeno natural, ya sea por el impacto de eventos EMP (pulso electromagnético)

[9] Véase, *Future Global Shocks,* http://www.oecd.org/dataoecd/24/36/48256382.pdf
[10] Véase, OECD/IFP Futures Project, en *Future Global Shocks, Geomagnetic Storms,* OCDE, 14-1-2011. http://www.oecd.org/dataoecd/57/25/46891645.pdf
[11] El segundo y tercer grupos de riesgos se pueden consultar en el documento de análisis del IEEE 17/2011, *Análisis comparativo de la Estrategia Española de Seguridad. «Una Responsabilidad de todos».*
[12] Informe *Developing Threats: Electro-Magnetic Pulses (EMP*). House of Commons Defence Committee, 22 febrero 2012.

provocados por dispositivos nucleares, cuyos efectos serían muy graves, aunque la probabilidad se considera actualmente baja. La probabilidad de que las tormentas geomagnéticas impacten sobre la magnetosfera terrestre se valora de moderado a alto en los próximos cinco años, con el potencial de provocar daños tanto a los sistemas de conducción eléctrica como a la red eléctrica[13].

Aunque el Registro de Riesgos Nacionales de 2010 no incluía una referencia explícita a la meteorología espacial o a eventos EMP, el Registro de 2011[14] sí lo incluye como un riesgo natural junto al riesgo volcánico (erupciones de nubes de cenizas y gases).

Existe un número de similitudes entre los efectos de un clima espacial inclemente[15] y un ataque EMP deliberado –sobre todo, en que ninguno respeta las fronteras nacionales– por ello el gobierno británico los ha tratado por separado.

El informe considera que la infraestructura crítica nacional de Gran Bretaña podría verse debilitada por un ataque espacial por terroristas o por un estado no respetuoso con las normas internacionales: un artefacto nuclear detonado a unos quinientos kilómetros sobre la superficie de la Tierra podría generar un pulso electromagnético, con un efecto «devastador» sobre los suministros de energía, telecomunicaciones y otros sistemas vitales.

Según el informe, los estadounidenses también concluyeron que, en el caso de un ataque, el colapso generalizado del sistema de energía eléctrica sería «prácticamente inevitable».

El informe establece que «La defensa consiste en la construcción de la resiliencia[16] de la infraestructura electrónica mediante la sustitución gradual, durante las tareas rutinarias de mantenimiento, de los sistemas, chips y conexiones increíblemente delicados y vulnerables por sistemas más resistentes, disponibles a un precio no muy caro».

El comité dijo que ahora es vital que el Gobierno se asegure que los procedimientos y equipos de respaldo estén preparados para enfrentarse a un «escenario razonable en el peor de los casos» producido por un fenómeno de inclemencia del clima espacial.

---

[13] La red nacional de suministro eléctrico ha estimado que si hubiera otro evento tipo Carrington, habría una posibilidad del 91% de que una zona del Reino Unido se quedara sin electricidad durante dos meses o más, al tiempo que los sistemas esenciales también podrían verse afectados.
[14] NRR, *National Risk Register of Civil Emergencies. 2012 edition.*
[15] Véase, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*, July 2008, Congressional Research Service.
[16] Ver nota 123. Referencia a la capacidad de resistencia y recuperación.

Muchos de los puntos que plantea este informe están ya coordinados por el Gobierno, y serán cubiertos por la Política Nacional de Seguridad Espacial que se espera a finales de este año.

LOS PELIGROS DEL CIBERESPACIO

Introducción

La Estrategia Española de Seguridad identifica el ciberespacio como uno de los seis ámbitos o entornos específicos donde tienen lugar las amenazas y riesgos más importantes para la seguridad de nuestro país: «Junto a los clásicos ámbitos terrestre, marítimo y aéreo, donde se han venido manifestando hasta ahora la mayoría de las amenazas y riesgos, otros como el espacial, el informativo y, singularmente, el ciberespacio cobran hoy una importancia capital».

La Estrategia define el ciberespacio como «el espacio virtual donde se agrupan y relacionan usuarios, líneas de comunicación, páginas web, foros, servicios de Internet y otras redes. Creado por el ser humano, es un entorno singular para la seguridad, sin fronteras geográficas, anónimo, asimétrico, que puede ser utilizado de forma casi clandestina y sin necesidad de desplazamientos. Es mucho más que la red, pues incluye también dispositivos como los teléfonos móviles, la televisión terrestre y las comunicaciones por satélite».

En este espacio se prestan servicios ampliamente utilizados por los ciudadanos, como los buscadores de información y el correo electrónico, pero también se proporcionan y gestionan muchos servicios e infraestructuras tanto privados como de las administraciones públicas.

La ciberseguridad puede verse comprometida por causas técnicas, fenómenos naturales o ataques intencionados e ilícitos. Los ciberataquesson una amenaza en crecimiento, cuyos posibles agentes -terroristas, crimen organizado, empresas, estados o individuos aislados- podrían poner en dificultad infraestructuras críticas.

El ciberespacio es asimismo un ámbito para el espionaje, incluido el económico, por parte tanto de agentes criminales como de otros estados; para ciberataques de terroristas, delincuentes e incluso de otros estados, aunque los más comunes tienen fines comerciales[17]. La obtención de información y de datos personales en la red, a menudo para ser vendidos a terceros, es cada vez más frecuente y preocupante.

La seguridad del ciberespacio no es un simple aspecto técnico, es un eje fundamental de nuestra sociedad y nuestro sistema económico. Los sistemas informá-

[17] Véase la Encuesta Global de Delitos Económicos 2011. *Cibercrimen: ¿Está su organización en riesgo?* PWC.

ticos cada vez son más importantes en la economía, la estabilidad y prosperidad económica del país, por tanto, estos dependerán en buena medida de nuestra ciberseguridad. No solo el coste económico, también hay que considerar la pérdida de confianza entre los ciudadanos ante un ciberespacio inseguro.

El carácter crítico de este espacio ante las vulnerabilidades convierte en vital su protección y su capacidad de resistencia y recuperación[18], además de fortalecer la legislación y fomentar la colaboración público-privada.

El ciberespacio es, además, otro de los dominios comunes (*global commons,* en inglés) al servicio de la humanidad como son la tierra, el aire, el mar y el espacio. El ciberespacio se considera también un entorno estratégico, por ello, está sujeto y lo estará aún más en el futuro, a tensiones por su dominio por parte de ciertos actores, como ha sucedido con los otros dominios.

En el ámbito concreto de las FAS y FCS[19], estas operan en red de forma creciente y son cada vez más dependientes de los sistemas de las tecnologías de la información y las comunicaciones (TIC) en campos como las comunicaciones, la meteorología, inteligencia, detección y seguimiento de misiles, vigilancia y exploración, posicionamiento y navegación. Son también, en consecuencia, mucho más vulnerables a la no disponibilidad, e incluso alteración de la confidencialidad e integridad, ya sea parcial o temporal, de esas capacidades. Tampoco hay que olvidar el riesgo de actuaciones similares de actores estatales y no estatales, o el posible uso del ciberespacio por parte de organizaciones terroristas, así como por el crimen organizado, gracias a su bajo coste. Su uso, simplemente supone un conjunto de ventajas apreciables[20].

Por tanto, la tensión y el conflicto están llegando también al ciberespacio, y lo hará con mayor intensidad en un futuro previsible. Ante esta realidad no cabe otra opción que, primero, realizar un análisis del riesgo que permita su identificación, estimar su ocurrencia para poder prevenirlo y determinar la actuación cuando un riesgo se ha materializado; segundo, cambiar los criterios fundamentales y las bases de regulación para evitar dar por supuesto muchas asunciones que probablemente ya no son válidas con los nuevos equilibrios de poder. Tras este cambio urge extremar dos aspectos que se presentan como determinantes. Primero, avanzar en lo posible en la regulación de las actividades, extremando el rigor en la vigilancia y exigencia de la normativa, lo que permitiría detectar y sancionar adecuadamente el «uso no responsable» del ciberespacio. Segundo, ahondar en el terreno de la cooperación y la complementariedad entre los diferentes actores, fomentando el multilateralismo en

[18] Ver nota 123.
[19] FAS, Fuerzas Armadas; FCS, Fuerzas y Cuerpos de Seguridad del Estado.
[20] El ejemplo del reducido y concreto efecto en el panorama internacional causado por el ataque a las instalaciones nucleares iraníes mediante el virus Stuxnet en 2010 es muy significativo, sobre todo, si se compara con el que hubiera ocasionado en caso de perseguir unos efectos similares mediante un ataque aéreo o de misiles.

el ciberespacio que permita construir un escenario de intereses comunes que pueda prevalecer sobre intereses particulares.

Los riesgos tecnológicos según la OCDE

Ya en 2011 la Organización para la Cooperación y el Desarrollo Económico (OCDE[21]), en el informe extraído del proyecto *Future Global Shocks*[22], señalaba que los ciberataques podrían causar catástrofes mundiales al igual que otros desastres. El informe sirve como prueba para demostrar cómo el sistema económico puede llegar a sufrir un *shock* global a gran escala debido a los ciberataques.

El estudio de la OCDE concluye que los ataques cibernéticos serán omnipresentes en las guerras del futuro, y que el armamento cibernético estará cada vez más desplegado y con un mayor efecto sobre los activistas de todas las tendencias ideológicas e intereses. El informe llega a la conclusión de que una verdadera «guerra cibernética», luchando casi en su totalidad a través de sistemas informáticos, es poco probable, ya que muchos de los sistemas críticos están bien protegidos y los efectos de los ataques serán difíciles de predecir, por lo que podrían volverse en contra de los agresores. No obstante, y complementando este estudio, si el agresor minusvalora las consecuencias de una guerra cibernética sobre sí mismo además de las consecuencias sobre el agredido, las probabilidades de este tipo de guerra se elevan.

Hay que puntualizar a este informe que según los datos de uso de Internet a finales de 2011 las regiones del mundo con mayor penetración de Internet son Norteamérica, Australia y Europa (78,6%, 67,5% y 61,3% respectivamente)[23]. Por tanto, una catástrofe mundial causada por un ciberataque sería matizable, ya que un ciberataque a gran escala impactaría en estas tres áreas del mundo. En cualquier caso, es cierto que los activos más importantes están dentro de sistemas informáticos (desde datos financieros y bancarios, datos empresariales, hasta datos personales) y por eso, posiblemente, el autor lo califica de «catástrofe mundial», aunque es poco probable ya que muchos de los sistemas críticos están bien protegidos», muchas veces no exponiéndolos directamente a Internet. Destaquemos que solo un 32% de los habitantes del mundo tiene Internet.

Los riesgos tecnológicos según el FEM

El Foro Económico Mundial (WEF[24], por sus siglas en inglés) publicó en enero el *Informe riesgos globales 2012*[25], en donde los ciberataques y los fallos

[21] OECD, por sus siglas en ingles, Organisation for Economic Cooperation and Development.
[22] Ver nota 130.
[23] Véase Internet World Stats, www.internetworldstats.com/stats.htm estimación a 31 de diciembre de 2011.
[24] World Economic Forum. Véase www.weforum.org
[25] Véase http://reports.weforum.org/global-risks-2012

en infraestructuras críticas se consideran dos de los cinco riesgos principales junto a otros tres, como el envejecimiento de la población, el cambio climático, y las diferencias económicas entre el primer y tercer mundo.

Esto supone un gran reto para las entidades públicas, las empresas privadas, y, en especial, para los profesionales de la seguridad de las TIC (tecnologías de la información y la comunicación), dentro de un mundo globalizado.

El informe, en su séptima edición, se basa en una encuesta realizada a 469 expertos de la industria, el gobierno, el mundo académico, y la sociedad civil e incluye una descripción más detallada de los riesgos y un análisis riguroso de datos que examina 50 riesgos globales repartidos en cinco categorías: económica, medioambiental, geopolítica, social y tecnológica.

Este informe introduce el concepto de «centro de gravedad», es decir, aquel riesgo considerado de mayor importancia dentro de las cinco categorías anteriores y alrededor del cual orbita el resto. Para una planificación orientada al riesgo, los centros de gravedad deberían servir como puntos focales para guiar las intervenciones y toma de decisiones de carácter estratégico.

De las cinco categorías mencionadas anteriormente, el centro de gravedad de la categoría tecnológica es el fallo de los sistemas o infraestructuras críticos[26]. Alrededor de este centro gravitatorio orbitan amenazas que incluyen ciberataques, fraude, robo masivo de datos y la desinformación digital a gran escala. Todos ellos han sido ponderados como de baja probabilidad, pero de un elevado impacto**.** Los ciberataques identificados por el FEM recogen desde los sabotajes sofisticados de alto nivel, normalmente sufridos por grandes corporaciones y gobiernos, hasta los ataques subversivos de bajo coste, a menudo perpetrados por los grupos de presión como Anonymous.

El informe destaca el efecto singular de un conjunto concreto de riesgos globales más que el efecto de un riesgo existencial único. De la revisión del conjunto de riesgos de este año surgen tres conjuntos o constelaciones distintas de riesgos que presentan una amenaza muy seria para nuestro futuro de prosperidad y seguridad, uno de estos conjuntos es el lado oscuro de la conectividad. Este caso describe la conexión entre una selección de riesgos globales, su interacción y su desarrollo probable en los próximos diez años. Inicialmente ,los casos se basan en un análisis cuantitativo de las

[26] Una infraestructura crítica comprende un conjunto de instalaciones, servicios y equipos de tecnología, cuya alteración tendría gran impacto en la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas. Existen multitud de infraestructuras que, aun no siendo críticas, su destrucción parcial o total tendría gran impacto en el bienestar social y en la confianza de los ciudadanos hacia la efectividad de las fuerzas de seguridad de un país. Algunas de estas infraestructuras son el sistema de transportes, de red eléctrica y el sistema de distribución de aguas.

interconexiones identificadas y posteriormente desarrolladas más mediante un análisis cualitativo.

Si bien el informe refleja que los impactos de la delincuencia,el terrorismo y la ciberguerra en el mundo virtual todavía no se igualan a las del mundo físico, existe un temor fundado y razonable de que esta situación pueda cambiar en el horizonte temporal de diez años.

La conectividad, el efecto esperado de la globalización, es una realidad. Con cerca de cinco mil millones de teléfonos móviles, conexión permanente a Internet y un número ingente y creciente de aplicaciones en la nube, la vida cotidiana es más vulnerable que nunca a las ciberamenazas y a la indisponibilidad de servicios TIC críticos. Esta conectividad tecnológica conlleva oportunidades, pero también riesgos, como es la mayor vulnerabilidad de los individuos frente a quienes les atacan maliciosamente de manera remota. La seguridad en el ciberespacio implica una necesidad urgente de fomentar el compromiso del sector privado, para reducir la vulnerabilidad de la información clave de los sistemas tecnológicos.

El informe formula cuatro sugerencias a los líderes mundiales para ayudar a reducir los riesgos de ciberataques. Estas medidas adaptadas al caso español serían:

a) Alinear el mercado: para que no solo los profesionales del sector, especialmente los proveedores, se preocupen por los ciberataques y sus riesgos, sino que los usuarios y las víctimas informen de los ataques sufridos y de ellos se aprenda. (Aplicado a nuestro país, se debería normalizar una formación universitaria para directores y técnicos en seguridad de una organización. Actualmente existen cursos cortos, cuyos contenidos no están acordes con la responsabilidad real de sus trabajos. Sería preciso determinar además su respaldo legal, qué responsabilidad real les otorga una organización: en la continuidad del negocio, ante una eventual pérdida económica si un ciberataque borra toda la información corporativa, etc. En este sentido, la Agencia Europea de Seguridad de la Información (ENISA) ha publicado un informe[27] que pone de relieve el hecho de que, a pesar de la preocupación por la ciberseguridad, la cobertura tradicional ofrecida por los proveedores de seguros de Europa no hace frente a los riesgos digitales.
b) Colaboración multisectorial: los gobiernos, el sector privado, civil y militar deben trabajar juntos, reconociendo que la inseguridad del ciberespacio es una amenaza para el resto del sistema. (El gobierno español, en su reciente Ley de Protección de Infraestructuras Críticas, solicita elaborar un plan de seguridad para cada una «sin que supongan incremento alguno del gasto público». En este escenario de crisis, la protección de las infraestructuras críticas, tanto física como lógica,es uno de los once riesgos de la EES).

[27] *Incentivos y obstáculos para el mercado del seguro cibernético.*

c) El mercado negro de los ataques (*exploits*, en inglés): hay que incentivar suficientemente el análisisde vulnerabilidades en el *software* comercial para contrarrestar el lucrativo mercado de venta de ataques que aprovechan vulnerabilidades.
d) Desarrollo de normas sociales en el ciberespacio: acciones no aceptadas socialmente en el mundo físico, como el robo o el espionaje industrial, se aceptan y se consideran normales en el ciberespacio; habría que investigar sociológicamente para entender por qué las normas sociales y éticas del mundo real no se traspasan al mundo virtual. (Agilizar la creación de normas que cubran ese vacío social y legal sin caer en el exceso de burocracia. La suplantación de identidad, que con frecuencia se da en este mundo virtual, plantea el dilema de incentivar o no el uso de identidades seguras mediante, p. ej., el DNI electrónico, y mantener la «falsa» sensación de anonimato como valor en Internet; sin embargo, el límite debe ser siempre el respeto a la legalidad).

Hoy en día entendemos mejor los beneficios de Internet y de la conectividad que sus riesgos. El terrorismo, el crimen y la guerra en el mundo virtual –hasta ahora– han sido menos mortales y «perturbadores» que sus equivalentes en el mundo físico. Los ciberataques van desde lo mundano y la pequeña delincuencia al fallo y parada de sistemas críticos, pudiendo, incluso, desencadenar la lucha armada física.

Hay que tener presente algunos axiomas de esta era cibernética:

- No existen sistemas informáticos 100% seguros y probados, solo sistemas cuyos fallos aún no han sido descubiertos, por lo que tratar de demostrar su infalibilidad es tan inútil como negar la gravedad.
- Cualquier dispositivo con *software* basado en el comportamiento del usuario puede ser manipulado para hacer cosas que sus creadores no tenían identificado.
- Cualquier dispositivo conectado a una red de cualquier tipo puede verse comprometido por un tercero. Aunque muchos de estos compromisos aún no se hayan detectado.
- La ciberseguridad es un problema que ninguna organización, pública o privada, puede resolver por sí sola.

Los directivos de las compañías aún siguen percibiendo las ciberamenazas como una cuestión técnica y no perciben el impacto de un ataque en el negocio. Las ciberamenazas son reales, y las empresas tienen que dedicar el tiempo y los recursos proporcionales al riesgo que afrontan.

En palabras del fundador y socio ejecutivo del Foro Económico Mundial, Klaus Schwab, «cuanto más complejo es el sistema, mayor es el riesgo de un fallo sistémico masivo, pero también mayor es el potencial de las oportunidades». Por tanto, se debe afrontar un cambio cultural tanto a nivel empresarial

local como a nivel sociopolítico global que permita reorientar las estrategias de negocio y protección desde una gestión a corto plazo de los riesgos más inmediatos a una aproximación global y colaborativa que permita ofrecer resistencia a los ciber-riesgos *(cyber-risk resilience*[28]).

Las amenazas a las infraestructuras críticas

Como ya se ha señalado anteriormente, los fallos de las infraestructuras críticas es un riesgo tecnológico señalado por la OCDE y el Foro Económico Mundial, la UE, así como por la EES.

La protección de las infraestructuras críticas se recoge en la legislación española con la Ley 8/2011 de Protección de las Infraestructuras Críticas[29]. Además de la ley y el reglamento que la desarrolla, se han elaborado unas guías con los criterios para los planes de seguridad de estas infraestructuras[30]. Mediante estas guías se insta a las empresas a equiparar en sus planes de seguridad la amenaza cibernética a los riesgos tradicionales de carácter físico. Al aplicar estos criterios se persigue conseguir una mejora global de la seguridad, basada en la colaboración, confianza y confidencialidad en el intercambio de información entre las instituciones públicas y las empresas privadas.

La amenaza cibernética a las infraestructuras críticas tuvo su más recordada materialización con el ataque del troyano Stuxnet[31] en 2010 a los sistemas de control de la central nuclear iraní de Bushehr. Esto supuso un retraso en el programa nuclear de Irán sin recurrir a un ataque militar y, por tanto, con menores riesgos y consecuencias, aunque también hubo efectos colaterales ya que

[28] Ver nota 123, referencia a la capacidad de resistencia y recuperación.
[29] La Ley 8/2011 establece medidas para la protección de las infraestructuras críticas. Se cuenta con el primer Plan Nacional de Protección de Infraestructuras Críticas (PNPIC) y el Catálogo Nacional de Infraestructuras Estratégicas, cuya custodia pertenece al Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC). Se ha desarrollado el Real Decreto 704/2011 con el Reglamento de Protección de las Infraestructuras Críticas.
Las infraestructuras críticas, según el PNPIC, se pueden dividir en 12 sectores estratégicos: Centrales y redes de energía; Tecnologías de la información y las comunicaciones; Sistema Financiero y Tributario (por ejemplo, banca, valores e inversiones); Sector sanitario; Espacio; Instalaciones de Investigación; Alimentación; Agua (embalses, almacenamiento, tratamiento y redes); Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico); Industria Nuclear; Industria Química; Administración (servicios básicos, instalaciones, redes de información, activos, y principales lugares y monumentos nacionales).
[30] El *Boletín Oficial del Estado* de 23 de noviembre de 2011 publicó la Resolución de 15 de noviembre de 2011, de la Secretaría de Estado de Seguridad, por la que se establecen los contenidos mínimos de los planes de seguridad del operador (PSO) y planes de protección específicos (PPE) conforme a lo dispuesto en el Reglamento de Protección de Infraestructuras Críticas. Véase www.cnpic.es
[31] Cuadernos de Estrategia, n.º 149, *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*. Instituto Español de Estudios Estratégicos. Ministerio de Defensa, diciembre 2010.

afectó a industrias de otros países que usaban el mismo sistema de Siemens atacado. En aquel momento, los expertos consideraron que Stuxnet era el primer *software* dañino capaz de penetrar en los sistemas automáticos de control de infraestructuras públicas, como centrales eléctricas y nucleares, presas e industrias químicas.

Este ataque y otros posteriores dirigidos a instalaciones industriales críticas[32] han aumentado los temores de una ciberguerra en la que las bombas lógicas serán programas dañinos que buscarán paralizar o destruir las conexiones y las infraestructuras críticas de un país anulando sus sistemas informáticos.

Las distintas estrategias nacionales de seguridad de los países de nuestro entorno han incluido o están incluyendo la ciberseguridad como uno de los aspectos a tener en cuenta. Muchos de estos países han desarrollado, incluso, una estrategia específica de ciberseguridad, como es el caso de EE. UU., Reino Unido, Francia, Alemania, Países Bajos[33], y organizaciones internacionales como la OTAN[34] y la UE[35], etc. En el caso de España, la estrategia de ciberseguridad es una de las peticiones recogidas en la EESy está en pleno proceso de desarrollo.

Según el Centro Criptológico Nacional los ataques más peligrosos provienen del llamado ciberespionaje, seguidos de los relacionados con el cibercrimen,

[32] Stuxnet evolucionó al gusano Duqu en 2011 cuyo objetivo era conseguir datos de las empresas. Según el responsable de la Seguridad de la Información de Gas Natural «hace unas semanas, poco antes de las elecciones generales, España, sufrió un ataque del virus Duqu que pudo haber puesto en jaque las infraestructuras críticas del país», «afortunadamente se detectó y se neutralizó». Con ciertas semejanzas a los dos anteriores, en mayo de 2012 se alertó sobre Flame, una herramienta de espionaje cibernético altamente sofisticada detectada contra objetivos de Oriente Próximo y Europa del Este. En agosto se detectaba el virus Gauss, capaz de espiar las transacciones bancarias y robar información de acceso a redes sociales, correo electrónico y mensajería instantánea, aunque según la empresa de seguridad informática Kaspersky Lab puede ir más allá atacando infraestructuras críticas.
Respecto al nuevo virus Flame se confirma que ha sido desarrollado conjuntamente por EE. UU. e Israel para recabar información para acciones de cibersabotaje contra el programa nuclear iraní. El esfuerzo corrió a cargo de la Agencia de Seguridad Nacional (NSA), la CIA y el Ejército israelí (IDF), quienes también crearon Stuxnet en la denominada operación Juegos Olímpicos. Todo esto se enmarca en la primera campaña sostenida de la historia de cibersabotaje contra un adversario de EE. UU., según informaba *The Washington Post.* Resulta sorprendente que estos países reconozcan abiertamente la realización de estos ataques y sabotajes contra otra nación soberana, o tal vez no tanto. Este tipo de actuaciones está provocando que muchos países estén adoptando contramedidas; en junio la Fuerza de Defensa Federal (Bundeswehr) alemana anunciaba por vez primera que posee una unidad secreta de guerra informática capaz de efectuar acciones ofensivas, que se estableció en 2006 y lleva operando desde entonces.

[33] ENISA, la Agencia Europea de Seguridad de la Información, presentó los documentos «*Estrategias de Seguridad Cibernética» de los Países Bajos, Francia y Alemania en marzo de 2011.*

[34] La OTAN, en la Cumbre de Lisboa celebrada el 20 de noviembre de 2010, aprobó la estrategia de ciberseguridad.

[35] Incluyendo la protección de las infraestructuras nacionales y europeas de información. Resolución del Parlamento Europeo de 12 de junio de 2012 sobre la protección de infraestructuras críticas de información, logros y próximas etapas: hacia la ciberseguridad global.

el ciberterrorismo y el activismo ideológico en la red, que es el más visible socialmente por las acciones de grupos como Anonymous. Se necesita tener una actitud proactiva[36] no solo reactiva, únicamente con medidas defensivas, y esto pasa por una solución integral (que englobe seguridad lógica y física) y por aumentar los recursos humanos y económicos. La futura estrategia de ciberseguridad deberá definir unas metas y objetivos claros, en la que se establezcan aspectos clave como: a quién se va a asegurar, contra qué amenazas, con qué medios técnicos, educativos, regulatorios y bajo qué modelo de financiación.

Internet de las cosas

La llamada «Internet de las cosas»[37] representa ya un futuro en el que los objetos cotidianos podrán recoger cómo transmitir información. Esto supone, sin duda, potenciales beneficios económicos y sociales que pronto se harán realidad, pero que habrán de combinarse con el respeto a la privacidad y la protección de los datos. De ahí la conveniencia de analizarlos previamente, garantizando, al mismo tiempo, un grado adecuado de control de los dispositivos de recogida, tratamiento y almacenamiento de la información.

Por este motivo la Comisión Europea ha iniciado un proceso de consulta pública para que la ciudadanía de la Unión Europea pueda opinar sobre el futuro «Internet de las cosas», con el objetivo de utilizar la información recopilada como base para la creación de un documento de recomendaciones al respecto. La finalidad es abordar el potencial económico y social del «Internet de las cosas» sin vulnerar la seguridad ni los derechos de privacidad de los ciudadanos.

Se calcula que en la actualidad el ciudadano medio dispone de al menos dos objetos conectados a Internet, se prevé que esta cifra será de siete en 2015, lo que supone, a escala mundial, 25.000 millones de dispositivos de conexión inalámbrica. En 2020 esa cifra podría duplicarse, situándose en 50.000 millones. Ello significa un futuro posible en el que muchos objetos cotidianos estarán

[36] Con continuos ataques de piratas informáticos a empresas, organizaciones y países de todo el mundo para hacerse con sus datos, el Gobierno de Japón trabaja en un nuevo proyecto creado para atajar ciberataques,que consiste en un programa capaz de rastrear la fuente de un ataque cibernético y neutralizarlo. *Emerging Cyber Threats Report 2011*. GTIC, Georgia Tech Information Center, Security Summit 2010. Tanto EE. UU. como China han puesto en marcha proyectos parecidos con este tipo de «armas» cibernéticas. Se trata de una prueba más de cómo los países están aumentando su inversión en desarrollar armas y medidas de seguridad informática.

[37] El llamado «Internet de las cosas», traducción literal del término inglés *Internet of Things* (IoT), se asocia al proceso de vinculación de cualquier objeto a un chip con dispositivo inalámbrico y dirección IP propia. No solo móviles y coches, sino también electrodomésticos, ropa, alimentos y cualquier bien o producto podrían tener, en el futuro, una conexión propia a Internet y, consiguientemente, una identificación propia.

conectados. Esto supondría poder modificar nuestra agenda cotidiana en tiempo real, adaptándonos a los eventos que sucedieran.

La Internet actual permite tener acceso a contenidos e información mediante la conexión a páginas weba partir de múltiples terminales, como ordenadores, teléfonos inteligentes o televisores[38]. El siguiente paso permitirá el acceso a información relacionada con el entorno físico, a través de objetos conectados que puedan captar información de su entorno y transmitirla a través de microprocesadores inteligentes que utilizan la identificación por radiofrecuencia (RFID).

Los peligros de la nube

La nube se puede considerar una evolución de los tradicionales centros de procesos de datos de una entidad hacia una nueva arquitectura de las infraestructuras TIC. La computación en nube (*cloud computing*)[39] constituye un modelo en auge de prestación de servicios de tecnología. La nube permite el almacenamiento en la red de los datos y los hace accesibles desde cualquier lugar.

Aún no existe una definición estándar aceptada universalmente. Nos podemos basar en la definición del Laboratorio de Tecnologías de la Información del NIST[40], que define la computación en nube[41] como: «Un modelo que permite un acceso ubicuo, práctico, bajo demanda a través de la red a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar rápidamente con el mínimo esfuerzo de gestión o interacción del proveedor del servicio».

[38] Sin embargo, están proliferando millones de aplicaciones (conocidas por su sigla apps) especializadas en pequeñas funciones pero con alto valor. Este fenómeno supone romper el equilibrio del acceso a la información bajo modelos normalizados y abiertos, como los navegadores, y promover el acceso a través de sistemas operativos propietarios, totalmente incomunicados entre sí, y que requieren soluciones distintas, pérdida de eficiencia y sobrecostes en el mejor caso. Se espera que la propia evolución de la conectividad conduzca a la aceptación e implementación de modelos abiertos y estándares como ha sucedido hasta ahora con los navegadores y con otras herramientas de acceso a la información.

[39] JOYANES, Luis (2009*a*). «La Computación en la Nube *(Cloud Computing)*: El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento», *Icade,* n.º 77, enero-marzo 2009. Madrid: Universidad Pontificia Comillas.

[40] National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología) es una Agencia del Departamento de Comercio de los Estados Unidos. Véase www.nist.gov Dentro del NIST, el Computer Security Resource Center (CSRC, Centro de Recursos de Seguridad Informática) elabora las normas sobre tecnologías de la información, entre ellas las relativas al *cloud computing*. Véase http://csrc.nist.gov

[41] The NIST Definition of Cloud Computing. NIST Special Publication 800-145, septiembre 2011.

La nube puede presentar diversas tipologías según la localización y la gestión de la infraestructura. La nube privada ofrece unos servicios a una entidad, y su infraestructura es íntegramente gestionada por una organización. La nube pública es operada por un proveedor que ofrece servicios al público en general. La nube híbrida, combina dos o más nubes individuales que pueden ser, a su vez, privadas o públicas, y permite portar datos o aplicaciones entre ellas.

Diversos estudios reflejan que cada vez más entidades públicas y privadas, desde grandes multinacionales hasta pequeñas empresas de ámbito local y administraciones públicas, utilizan sistemas de computación en nube en alguna de sus modalidades, debido a las ventajas que puede proporcionar en términos de ahorro, alta disponibilidad, adaptabilidad, fiabilidad y control de acceso seguro a los datos entre otras.

La tendencia en la nube apunta hacia la movilidad y la ubicuidad. Los usuarios de telefonía móvil y los usuarios de Internet continúan creciendo. La gran mayoría de estos usuarios se conectan ya a la nube para descargarse programas y aplicaciones web desde cualquier lugar, en cualquier momento y con cualquier dispositivo, la llamada nube móvil[42]. Esto permitirá la ubicuidad del usuario pero también debe enfrentarse a amenazas de tipo cibernético.

Dado que la computación en nube no permite a los usuarios poseer físicamente los dispositivos de almacenamiento de sus datos (con la excepción de poder copiar los datos a un dispositivo externo), deja la responsabilidad del almacenamiento de datos y su control en manos del proveedor. También se cuestiona la limitación de la libertad de los usuarios y la dependencia del proveedor de servicios.

En este escenario de proliferación de servicios de computación en nube se suscitan en la actualidad interrogantes sobre las garantías aplicables en el marco de estos servicios, y la adecuación de las normas de seguridad, protección y priva-

[42] La tecnología inalámbrica (wifi, bluetooth, GSM, 3G, UMTS, etc.), sin duda, facilita la vida cotidiana de las personas permitiendo que los usuarios ya no dependan de un cable para poder utilizar servicios en Internet a través de sus teléfonos inteligentes y sus equipos portátiles. No obstante, esta tecnología también permite a terceros interceptar la información que el usuario transmite de forma más sencilla que en redes por cable, cuestión a la que se suma la extensa cantidad de redes wifi públicas e inseguras. Algunos riesgos posibles son el robo de archivos personales o de credenciales de acceso a bancos, redes sociales u otros servicios, vulnerabilidades en los mecanismos de cifrado GSM, técnicas para establecer falsas estaciones 3G, control remoto de dispositivos que emplean bluetooth/wifi, envío de mensajes manipulados dando órdenes de compra, órdenes de ataque en el contexto militar, etc. Por eso es importante que los usuarios tomen conciencia de esta problemática e implementen buenas prácticas para proteger la información.

cidad[43][44][45][46] de los datos a estos entornos se ha convertido en una cuestión esencial que está siendo objeto de análisis y evaluación en distintos ámbitos.

En la informática tradicional, tal y como la conocemos hasta ahora, las empresas y los usuarios conocen perfectamente dónde está su información almacenada localmente. Sin embargo, la empresa o el usuario de la nube no conocen con exactitud dónde está guardada su información. Esto supone confiar a terceros la seguridad de nuestros datos. Aspectos preocupantes en las nubes son la confidencialidad de la información, la disponibilidad del servicio y la portabilidad de los datos y procesos. Respecto a la confidencialidad de los datos, es importante no solo el contenido de la comunicación, sino también los metadatos asociados al tráfico: localización geográfica de los comunicantes, su identidad, información sobre los dispositivos conectados, volumen de información transmitida por un actor, etc. Esta metainformación es aún más interesante en la nube móvil.

Otra preocupación es el uso masivo de los servicios de la nube proporcionados por unos pocos proveedores, que supone la concentración en unos pocos puntos singulares de gran parte de los procesos que realizan entidades (públicas y privadas) en España.

Cuando los grandes proveedores de servicio están ubicados total o parcialmente fuera de España, algunos de ellos con una posición dominante en el mercado, plantean otros riesgos de tipo legal o de soberanía.

[43] La Agencia Española de Protección de Datos (AEPD) abrió el pasado enero una consulta pública sobre las implicaciones en materia de protección de datos de los servicios de Computación en Nube con el objetivo de recabar opiniones, perspectivas y experiencias, principalmente de prestadores y usuarios de servicios de computación en nube, así como analizar el grado de conocimiento y la aplicación práctica de estos servicios en España.

[44] Algunos países como EE. UU. ya han publicado una *Guía* de seguridad y privacidad para 'cloud c*omputing'* con los requisitos de seguridad para la nube. Esta publicación proporciona una visión general de los problemas de seguridad y privacidad que conlleva la nube pública y señala los aspectos a considerar por las organizaciones cuando utilizan este entorno para externalizar los datos, aplicaciones e infraestructuras. NIST Special Publication 800-144. *Guidelines on Security and Privacy in Public Cloud Computing.* Wayne JANSEN and Timothy GRANCE, diciembre 2011.

[45] La Unión Europea está trabajando en una Estrategia Europea para la computación en nube que espera publicar a lo largo de 2012. La Agenda Digital Europea ya contemplaba la computación en nube entre las tecnologías y tendencias estratégicas. La Agencia Europea de Seguridad, ENISA (www.enisa.europa.eu) ya publicó en enero de 2011un informe sobre *Seguridad y resistencia en las nubes de la Administración Pública.*

[46] En España INTECO (Instituto Nacional de Tecnologías de la Comunicación), basándose en el informe de ENISA, ha elaborado el informe *Riesgos y amenazas en el 'cloud computing'* con objeto de facilitar una visión general de amenazas, riesgos y aspectos a considerar en la seguridad en la nube. Estos informes se centran en aspectos de la gestión de los datos, fundamentalmente en la propiedad de los mismos y la forma de operarlos y tratarlos por parte del proveedor. Este informe está disponible en: http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

Siguiendo las indicaciones de la EES, no son solo los factores tecnológicos los que incrementan las posibilidades de que las ciberamenazas se materialicen, sino también los legales.

La prestación de un servicio está obligado por las leyes nacionales de dos maneras: obligan a unas garantías mínimas de seguridad y de confidencialidad (independientemente de lo estipulado por contrato), y facultan a las autoridades locales al acceso a la información, con mayor, menor o ningún control judicial, e imponen unas obligaciones de conservación de datos.

Pero no todos los países ofrecen las misma garantías por ley[47], algunos muy pocas y otros, aunque ofrecen unas garantías jurídicas y técnicas elevadas, también disponen de los recursos legales necesarios para saltarse las políticas de seguridad de cualquier proveedor de la nube.

Por ejemplo, en EE. UU., en aplicación de la ley antiterrorista Patriot Act, las autoridades norteamericanas pueden inspeccionar los datos almacenados o procesados por una compañía de su país aunque estén en un servidor físicamente alojado en otro territorio[48].

Por todas estas cuestiones, algunos expertos ya empiezan a considerar la computación en nube como una infraestructura crítica.

Peligros en la administración electrónica española

El Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT[49], adscrito al Centro Nacional de Inteligencia, CNI, recientemente publicó su resumen de amenazas de 2011 y las predicciones de seguridad de 2012, recogidas en su último informe *Ciberamenazas 2011 y tendencias 2012*.

Según dicho informe, durante el último año 2011 los ataques dirigidos contra diferentes organismos de la Administración Pública española han incrementado su número y, lo que es más preocupante, su nivel de criticidad (más de 90 incidentes de nivel muy alto o crítico). La introducción de código dañinoen los sistemas, las intrusiones mediante ataques a páginas webcon el fin de robar información, así como el contacto con direcciones IP maliciosas, son algunos de los incidentes más recurrentes sufridos por nuestras administraciones. También se observa, a nivel general, el avance del ciberespionaje, cuyo origen hay que buscarlo tanto en las empresas como en los propios estados (la cada vez mayor

[47] En España la transferencia internacional de datos está regulada genéricamente por la Ley de Protección de Datos.
[48] El Gobierno francés que preside Nicolás Sarkozy destinará, de momento, 135 millones de euros a crear su propio sistema de nube en Internet. El proyecto Andrómeda busca crear la alternativa francesa a este servicio para evitar que datos sensibles sean albergados en otros países. *El País,* 27/9/2911.
[49] CCN-CERT se puede consultar en www.ccn-cert.cni.es

presencia en formato electrónico de información muy valiosa y la dificultad técnica y jurídica de atribuir la responsabilidad no hace sino incrementarlo); la evolución delactivismo ideológico en la red (conocido como *hacktivismo*)y la colaboración entre el activismo tecnológico y el activismo físico; la evolución de untroyano bancario y su extensión por Internet; los ataques contra sistemas de autenticación y modelos de confianza; o la aparición del código dañino como servicio (llamado*malware-as-a-service* MAAS)mediante el cual los autores decódigo dañino (llamado *exploits,* escrito con vistas a utilizar un error del sistema y poder así tomar control de la máquina*)*, además de suministrarlos a sus clientes, ofrecen servicios adicionales como adaptaciones del código «a medida», servidores de mando y control o infección y explotación en remoto de objetivos seleccionados.

La tendencia para 2012 se orienta, entre otros puntos,a quelos activistas de la redextenderán sus objetivos; continuarán los ataques contra autoridades de certificación; se detectarán nuevas familias de código dañino y se potenciará la figura del intermediario (encargada de encontrar clientes que compren datos previamente robados). De igual modo, los peligros en las redes sociales, los dispositivos móviles, los servicios de la nube y los ataques de denegación de servicio distribuido (DDoS), incrementarán su número y la eficacia de los ataques. Asimismo, es previsible que las vulnerabilidades de aplicaciones en los navegadores (*add-ons:* componentes de terceros) cambien el enfoque, construyendo códigos que ataquen directamente a las vulnerabilidades de los propios navegadores, al objeto de instalar código dañino.

Por todo ello, y en opinión del CCN-CERT, el gran desafío para las organizaciones (administraciones públicas o sector privado) en el 2012 será mantener su capacidad para detectar y atajar problemas de seguridad de tecnologías de la información y ser capaces de adoptar nuevos métodos, procedimientos y herramientas para ello. A medida que se avance en el formato *on-line* de los procedimientos administrativos y empresariales, y la información sea accesible, no importa desde qué lugar o a través de qué dispositivo, las herramientas de seguridad tendrán que seguir el ritmo, si se quiere mantener un nivel de seguridad razonable. No hay que olvidar que los ciberdelincuentes continuarán acechando a las presas más fáciles o más desprotegidas como un medio para alcanzar sus últimos objetivos. Por tanto, reducir los riesgos en el ciberespacio pasa necesariamente por incorporar mecanismos de defensa que tengan en cuenta las motivaciones y los incentivos de los atacantes.

El informe resalta la necesidad de impulsar una estrategia nacional de ciberseguridad en España (en desarrollo) con la que articular una respuesta adecuada, similar al resto de países de nuestro entorno. Constituye el mejor camino para desarrollar coherentemente todas las acciones de prevención, detección y respuesta que requieren las amenazas en el ciberespacio.

La adquisición de productos inseguros

Otro problema que se plantea con la externalización de la producción de dispositivos electrónicos es la falta de garantía sobre los mismos, ya sea el *hardware* y/o el *software* puede esconder puertas traseras que permitan el acceso remoto con total desconocimiento del usuario que adquiere ese dispositivo. Un ejemplo real lo tenemos recientemente en la cancelación de la compra de iPads por EE. UU. para sustituir los mapas de navegación por tener tecnología rusa.

En concreto, el Mando de Operaciones Especiales de la Fuerza Aérea estadounidense (AFSOC, por sus siglas en inglés) planeaba equipar a sus tripulaciones con carteras de vuelo electrónicas, para así eliminar los mapas de navegación y los manuales técnicos en papel y sustituirlos por versiones digitales almacenadas en tabletas iPad de Apple, que se entregarían a cada miembro de la tripulación. Esta sustitución del papel por los iPad era similar a la que estaban realizando varias líneas aéreas.

Tras tres meses de evaluación, según la Fuerza Aérea, solo la tableta de Apple satisfacía los requisitos del citado Mando. Además, la citada tableta se iba a equipar con un *software* de cifrado que aparentemente cumplía las exigencias de seguridad de las misiones. En concreto se seleccionó el *software* GoodReader, de Good.iware, para cifrar los archivos individuales, para asegurar que los datos estarían seguros incluso si un iPad o iPhone se perdiese o fuese robado. Además, serían equipados con comunicaciones Wi-Fi para actualizar los manuales.

El objetivo era usar tabletas y equipos móviles para aumentar la productividad de las misiones, disminuir los costes y lograr beneficios adiciones de portabilidad y flexibilidad. Además, se disminuirían la gran cantidad de papel que suponen los manuales técnicos y las cartas de vuelo que lleva cada avión, unos 32 kg.

Sin embargo, la compra se canceló porque los iPad llevarían tecnología rusa. El AFSOC recibió muchas críticas, porque sus pilotos, en misiones especiales, iban a utilizar un *software* desarrollado en Rusia.

Esto refleja la globalización de la industria de tecnologías de la información, cuando las compañías locales no pueden desarrollar y suministrar *software* crítico. Sin embargo, en estas aplicaciones críticas para el cumplimiento de las misiones, debería examinarse cada una de las líneas del código fuente para asegurar que no contengan códigos maliciosos, que podrían tener consecuencias muy graves.

Este caso refleja también la preocupación por mantener la seguridad en la cadena de suministro del *software.* Una vía para evitar estas inseguridades en

la cadena de suministros *hardware* y *software* es exigir una certificación de seguridad internacionalmente reconocida de los componentes de un sistema, sobre todo, cuando en este mundo global los componentes se fabrican fuera de las fronteras de un país.

La EES muestra su preocupación por la dependencia externa en sectores estratégicos, y en particular por la dependencia tecnológica, de forma que una de sus líneas de actuación es «Apoyar el desarrollo de empresas privadas nacionales en un sector estratégico como este, en el que puede ser peligrosa la dependencia de empresas extranjeras», y en especial «reduciendo la dependencia de la tecnología de seguridad de terceros países».

Otros peligros

El resultado de la creciente y acelerada evolución de la comunicación es que hoy nos enfrentamos al fenómeno de la «hiperconectividad»[50]. Este término se refiere no solo al millar de medios de comunicación y de interacción, sino también a su impacto en el comportamiento personal y organizativo. La hiperconectividad permite conexión permanente, grabación continua, fácil acceso, abundancia de información, interactividad, etc.

La hiperconectividad nos enfrenta con beneficios y desafíos. Puede ser una herramienta poderosa de colaboración que conduce a la alineación global (pero vigilando que no sea «alienación global»), a un aumento de la eficiencia, y al desarrollo material. Al mismo tiempo, ha cambiado muy rápidamente la manera de realizar muchas tareas y se espera que la gente se adapte a estos cambios. Sin embargo, debe vigilarse que no nos convirtamos en esclavos de la conectividad o cualquier otra tecnología.

Las tecnologías de la comunicación y la hiperconectividad se han convertido en un factor clave para los movimientos sociales de todos los tipos: las movilizaciones que causaron disturbios en algunas ciudades del Reino Unido en 2011 estuvieron coordinadas por mensajes de texto, por Facebook, Twitter, y servicios de Blackberry, Messenger; sin embargo, las mismas tecnologías ayudaron a impulsar la reunión de los grupos de oposición en la plaza Tahrir, de El Cairo, en 2011. Otro modo de compartir la información son los canales IRC, utilizados p. ej., por los activistas de Anonymous, que utilizan sus propios servidores, de manera que ninguna empresa controla la información que comparten.

Otro aspecto a considerar es la «deformación de la realidad» a que estamos sometidos. Por una parte, existe un exceso de información disponible, la llamada «infoxicación» (de información e intoxicación); por otra parte, cualquiera puede divulgar un mensaje; ambos hechos producen un riesgo evidente de manipulación. En un mundo interconectado, la realidad es que la gente se agrupa

[50] Véase www.weforum.org

con aquellos que le son afines y el resultado final es la «creencia de estar globalizado», pero cada uno ve la realidad «que quiere ver», porque es la de su grupo afín. Incluso en este mundo la gente se vuelve más crédula que en el mundo real, dando credibilidad a noticias de cuya fuente desconoce la identidad real y su grado de fiabilidad. Los buscadores de información y las redes sociales también pueden distorsionar la visión o percepción que tenemos de la realidad. Algunos buscadores emplean decenas de parámetros para decidir cómo ordenar las búsquedas y esto hace que los resultados de esas búsquedas no sean iguales para todos, con lo cual nos muestran realidades diferentes a cada uno. Esta tendencia además va en aumento.

La «democratización de la tecnología»: en los últimos años el acceso a la construcción de SW, HW, como incluso de piezas físicas (con las impresoras 3D), permite a casi cualquiera construir cosas que antes solo se podían comprar. Esto es un gran avance, pero también un riesgo evidente, porque permite a cualquiera construir virus, dispositivos de espionaje, armas, etc. En el fondo, es parecido a lo que pasó hace unos años con la polémica de que cualquiera podía obtener en Internet las instrucciones para construir una bomba.

BIOTECNOLOGÍA

Avances y posibles riesgos

En los últimos cincuenta años se han sucedido rápidos avances en el campo de la ciencia y la tecnología relacionados con desarrollos biológicos[51][52].Estos desarrollos, por una parte, mejoran el bienestar humano, pero, por otra parte, proporcionan un arma poderosa a estados y grupos terroristas. La facilidad de obtención y la disponibilidad de los materiales para producir armas biológicas, así como de los manuales y guías para su manejo, son pruebas de que el temor creciente entre la población no es infundado. También los servicios de seguridad y los servicios médicos tratan de estar preparados para las posibles consecuencias de un suceso de este tipo.

En el décimo aniversario de los ataques del 11-S surgieron algunas reflexiones, entre ellas la amenaza de las bioarmas debido a su carácter único: la exposición a mínimas cantidades de un agente biológico puede pasar desapercibido, para al final ser la causa de enfermedad o la muerte; el período de incubación de un agente microbiano puede ser de días o semanas; al contrario que un atentado o un bombardeo, un corte con un cuchillo o una dispersión química, un bioataque no podría reconocerse hasta tiempo después de la liberación del agente.

[51] «The Toxicology of Bioregulators as Potential Agents of Bioterrorism». Bokan S. Arh Hig Rada Toksikol 2005, 56:205-211, junio 2004.
[52] «Military Medical Readiness for Chemical and Biological Terrorists' attacks». Rostislav KOSTADINOV y otros autores. Military Medical Academy, Sofia, Bulgaria. *JMedCBR,* vol. 8, 2010, febrero 2010.

Según esto, el bioterrorismo[53] plantea distintos desafíos para estar preparados ante la protección y la respuesta.

A lo largo de la historia militar, algunos cambios tecnológicos han proporcionado nuevas armas y capacidades a los mandos militares. Algunos de estos cambios eran tan importantes que, en el caso de las armas nucleares, modificaron las posiciones estratégicas de los países que las tenían dentro del sistema internacional. Aunquelas armas biológicas no pueden destruir infraestructuras civiles o militares, pueden matar gente en gran magnitud. Como los efectos de la diseminación de armas biológicas son invisibles, retardados e inciertos, las armas biológicas modificadas genéticamente (ABMG)[54] pueden adquirir una capacidad de disuasión que presentaría serios desafíos a los gobernantes.

Hasta ahora, las armas biológicas se habían considerando incapaces de disuadir a los estados con armas nucleares. Sin embargo, los desarrollos recientes en biotecnología pueden alterar este escenario. Existen varias razones.

Primero, la biotecnología permite la transferencia de genes en patógenos que pueden hacerles resistentes a la radiación ultravioleta u otros efectos ambientales perjudiciales. Otros tipos de manipulación genética pueden hacerles también más resistentes a variaciones de presión y temperatura durante el vuelo o la explosión de un misil[55]. Anteriormente, la supervivencia de los patógenos después de su diseminación era un gran problema para los planificadores militares. Al conseguir los agentes biológicos alcanzar sus objetivos, la biotecnología los convierte en armas más previsibles.

Segundo, las contramedidas médicas que podrían usarse en un ataque con bioarmas podrían volverse casi inútiles. Por ejemplo, la inserción de genes resistentes a antibióticos en patógenos puede disminuir de manera importante el papel de los antibióticos en la biodefensa. Los científicos soviéticos desarrollaron patógenos, responsables de la plaga del ántrax, resistente a varios tipos de antibióticos. Con las vacunas sucedió lo mismo. Técnicas como la modificación de la estructura antigénica de un patógeno puede eliminar cualquier problema que las vacunas planteen a la dispersión de armas biológicas.

---

[53] Bioterrorism: Still a Threat to the United States. By Leonard A. COLE. *CTC Sentinel,* vol. 5, issue 1, enero 2012.

[54] «Biotechnology and Biological Weapons: Challenges to the U.S. Regional Stability Strategy». Francisco GALAMAS. Forum Intelligence. Portuguese Catholic University, Portugal. *Comparative Strategy*, 28:164-169, 2009, Taylor & Francis Group, LLC.

[55] Generalmente, las dos principales amenazas químicas y biológicas provienen de naciones hostiles que utilicen misiles o bien de grupos terroristas que usen dispositivos para liberar agentes químicos o biológicos. Véase Chemical and biological defense. *Updated Intelligence, Clear Guidance, and Consistent Priorities Needed to Guide Investments in Collective Protection,* GAO, United States Government Accountability Office, enero 2007.

Tercero, los agentes biológicos pueden manipularse para ser más contagiosos y letales, de modo que aumenten los efectos perjudiciales inaceptables que plantean estas armas[56].

Cuarto, nuevos tipos de armas biológicas, como agentes biológicos falsos, pueden crear un alto grado de incertidumbre y víctimas en un estado oponente. Estas capacidades, combinadas además con una alta capacidad letal, pueden hacer que el E

estado que posea estas armas biológicas plantee la amenaza de un daño inaceptable sin que se plantee el verdadero riesgo de la eficiencia de ese bioataque.

Estas armas serían más previsibles y letales mientras que serían más inmunes a las biodefensas existentes. Basándose en estas razones, y si solo se consideran las capacidades de esta arma, se puede decir que la biotecnología puede hacer que un estado con armas biológicas cree una disuasión efectiva como la de los estados nucleares.

De hecho, se puede establecer cierto paralelismo entre las armas biológicas modificadas genéticamente y las armas nucleares. Estos dos tipos de armas tienen un efecto aniquilador similar: algunas armas biológicas o bioarmas tienen un radio de acción más amplio que la radiación de origen nuclear; ambos tipos de armas contaminan durante décadas los territorios; su manipulación y producción conllevan un alto riesgo. Algunas características de las bioarmas superan a las armas nucleares desde su interés político y militar: no afectan a las infraestructuras de la zona de aplicación, sino solamente a su población humana; si el agresor dispone de una vacuna efectiva, entonces puede ocupar el territorio conquistado independientemente de la contaminación biológica. Esto supone una ventaja respecto al arma nuclear, por ello no es descartable que en un futuro cercano los proyectos y centros de investigación dedicados a las bioarmas proliferen en todo el mundo.

Otro aspecto de estas nuevas bioarmas es la facilidad de producción y la dificultad de detección del proceso de producción de estas armas. Esto permite que un estado que desea producir armas biológicas lo haga sin ser detectado, al contrario de lo que sucede con las armas nucleares. Si se comparan las fases de producción de bioarmas y armas nucleares es fácil comprender las diferencias. De las fases de producción de armas nucleares, la fase de enriquecimiento de uranio es altamente detectable mediante el uso de instrumentos de medida en satélites y otras plataformas. Con los programas de armas biológicas sucede lo contrario. Debido a la naturaleza dual, tanto del equipo como del conocimiento

[56] Un equipo de investigadores del Armed Forces Institute of Pathology de Maryland fue capaz de aumentar la virulencia del virus de la gripe incorporando en su genoma genes del virus que causó la epidemia de 1918. Alexander KELLE, Kathryn NIXDORFF, and Malcolm DANDO, *Controlling Biochemical Weapons: Adapting Multilateral Arms Control for the 21st Century.* New York: Palgrave Macmillan, 2006, pp. 80-82.

involucrados en la producción de estas armas biológicas, la detección de programas de este tipo de armas es extremadamente difícil[57]. Por el contrario, la detección temprana de los programas nucleares permite a la comunidad internacional tomar decisiones económicas, diplomáticas y militares para tratar el desequilibrio regional que estos tipos de armas crean.

Este aspecto, junto con el mayor poder letal, mencionado anteriormente, hacen de las bioarmas modificadas genéticamente candidatas a ser consideradas armas de destrucción masiva (ADM[58]), y, por ello, pueden tener repercusiones en la estabilidad regional.

La comunidad internacional, si quiere ser una fuerza estabilizadora en diferentes regiones del mundo, tendrá que reforzar su presencia en esas mismas regiones. Esto solo puede aumentar el coste financiero, militar y político de esa presencia.

Dos cuestiones a considerar, como sucede con otro tipo de armas, son los siguientes:

Vigilar una posible proliferación de este tipo de bioarmas. La proliferación de un arma de destrucción masiva alimenta los avances tecnológicos de esa arma. Lo contrario también es cierto. Solo manteniendo el liderazgo tecnológico algunos países pueden mantener su seguridad o su estatus. Por otra parte, los avances tecnológicos crean mayores niveles de capacidades militares, que a su vez influyen en el proceso de proliferación. En el caso particular de ABMG (armas biológicas modificadas genéticamente) puede surgir una carrera armamentística cuantitativa y cualitativa. Unos estados pueden iniciar programas de bioarmas avanzadas porque aspiran a las ventajas estratégicas alcanzadas por los países que ya tienen estas bioarmas, mientras estos últimos pueden sentir la necesidad de mejorar su arsenal de bioarmas para mantener su liderazgo tecnológicos. Esto puede incluir el desarrollo de nuevas y mejores bioarmas o nuevas contramedidas que anulan los efectos de las bioarmas del oponente.

Barajar la posibilidad de que estados con capacidad de producir ABMG se los proporcionen a grupos terroristas. Al suministrarles este tipo de armas, el estado proveedor pretende que estos grupos lleven a cabo acciones compatibles con sus intereses. Este tipo de estrategia normalmente produce resultados a medio/largo plazo porque pretende reforzar la retirada de la comunidad internacional de diferentes regiones del mundo aumentando el coste humano, material, financiero y político de la presencia regional. Si aumenta el poder

[57] Por ejemplo, tras la primera guerra del Golfo los inspectores de la Comisión Especial de las NN. UU. (UNSCOM) tardaron cuatro años en descubrir la verdadera dimensión del programa de bioarmas iraquí. Solo fue posible por la deserción del director, por entonces, de la industria militar iraquí.

[58] WMD, por sus siglas en inglés, Weapons of Mass Destruction.

mortífero y la resistencia de estas bioarmas, sus efectos pueden aumentar los costes de la presencia regional más rápidamente que con actividades terroristas convencionales.

Control de las armas biológicas

El esfuerzo en biodefensa ha producido avances considerables en entender la bioamenaza, en el desarrollo y ubicación de nuevas tecnologías de detección y en el aumento de la provisión de contramedidas. El aumento del número de laboratorios de alta seguridad y su personal plantean también un riesgo potencial.

Hay laboratorios por todo el mundo que están investigando desarrollos biomédicos, para el control de enfermedades infecto-contagiosas, tanto en el campo del diagnostico como el de la prevención (desarrollo de nuevos medicamentos y vacunas).

Algunos de estos laboratorios son sospechosos de tener una investigación de doble uso, como son el desarrollo de armas biológicas.

Están pendientes de implementar las recomendaciones de la comisión de la Convención sobre Armas Biológicas y Toxinas[59], que servirían para racionalizar la bioseguridad internacional. Se aboga por una estrecha vigilancia de todos los campos de la biotecnología a nivel mundial con objeto de aplicar medidas que puedan, si no eliminar, reducir la amenaza.

La mayoría de los gobiernos justifican sus investigaciones sobre guerra biológica como de naturaleza defensiva, cuestión permitida por el Tratado sobre Armas Biológicas, aun reconociendo que es prácticamente imposible distinguir en este campo entre investigación ofensiva y defensiva.

La gestión de las consecuencias de ataques químicos, biológicos, radiológicos, nucleares o con explosivos (CBRNE)[60] es un tema que se sitúa en la intersección de tres caminos sinuosos: la propagación del terrorismo trans-

[59] En 1972 se creó la Convención sobre Armas Biológicas y Toxinas (Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological –Biological– and Toxin Weaponsand on Their Destruction, BTWC, véase www.opbw.org) y entró en vigor en 1975. En la actualidad, 165 países la han ratificado y 12 la han firmado, pero no la han ratificado. Esta Convención prohíbe el desarrollo, producción y almacenamiento de este tipo de armamento. La «VII Conferencia de Examen de la Convención de Prohibición de Armas Bacteriológicas y Toxínicas1» (CABT) se celebró en Ginebra del 5 al 22 de diciembre de 2011. Sus resultados fueron muy limitados, ya que no se dieron pasos relevantes en ninguna de las cuestiones fundamentales para reforzar las garantías de cumplimiento.

[60] También se usa el acrónimo NBCR (nuclear, biológico, químico, radiológico o CBRN attacks). Véase «Improvised NBCR attacks on civilian and military and infrastructure». Peter D. ZIMMERMAN. *Defence against Weapons of Mass Destruction Terrorism.* IOS Press, 2009.

nacional; la proliferación de armas nucleares, y el avance y difusión de la biotecnología[61].

Esta nueva era, al contrario de la primera era nuclear de 1945, se caracteriza por estar en un mundo de fronteras nacionales porosas y un comercio extendido potencialmente peligroso en tecnologías y materiales de doble uso. Sin embargo, este período de globalización coincide con un desgaste de los acuerdos y normativas mundiales que mantuvieron a raya la proliferación de armas nucleares durante décadas[62].

Las voces de algunos expertos se alzan para animar un debate internacional sobre el papel potencial de la biotecnología en la defensa y la seguridad nacional, y abogan por aplicar medidas de control específicas para prevenir la fabricación de armas, como por ejemplo, mediante una ampliación de la Convención sobre Armas Biológicas, con un protocolo de verificación similar al que se aplica para las armas biológicas convencionales.

NANOTECNOLOGÍA

Introducción

La nanotecnología o nanociencia[63] es un campo de las ciencias aplicadas dedicado al control y manipulación de la materia a una escala de nanómetros (el equivalente a la mil millonésima parte de un metro o 10^{-9} metros). Los nanomateriales son sustancias o materiales químicos fabricados y utilizados a escala muy pequeña, en un rango de uno a cien nanómetros[64].

A esta escala la materia muestra propiedades inusuales –como propiedades catalíticas, eléctricas, magnéticas, mecánicas, ópticas y térmicas– que difieren de forma importante de las que muestran los materiales a escala convencional. Algunas de estas propiedades nuevas tienen su aplicación en muchos y variados sectores, como la electrónica, medicina, sociedad de la información, transporte, espacio, defensa y seguridad[65], ejemplos de ellos son pilas, baterías, recubrimientos, tejidos antibacterianos, material deportivo, etc.

---

[61] «CBRNE Consequence Management». David HEYMAN. *Military Technology. MILTECH,* 11/2009.

[62] *Bulletin of the Atomic Scientists,* enero/febrero 2007.

[63] El ganador del Premio Nobel de 1965, Richard Feynman, planteó la idea de nanociencia y nanotecnología en su discurso en el Instituto Tecnológico de California en 1959 titulado «En el fondo hay espacio de sobra (There's plenty of room at the bottom)».

[64] A modo de ilustración, una hoja de papel tiene un grosor de 100.000 nm, un cabello humano unos 80.000 nm y una fila de tres átomos de oro sobre 1 nm.

[65] El mercado mundial de productos relacionados con la nanotecnología está creciendo y se espera que alcance entre 1 y 2,6 billones de dólares en 2015. GAO (U.S. Government Accountability Office): Nanotechnology: *Nanomaterials Are Widely Used in Commerce, but EPA Faces Challenges in Regulating Risk;* mayo 2010, GAO-10-549.

Los nanomateriales tienen el potencial de mejorar la calidad de vida y contribuir a la competitividad industrial. Sin embargo, estos nuevos materiales también plantean riesgos para el medio ambiente, la salud y la seguridad física. El alcance de estos riesgos depende de la combinación de la toxicidad y la vía y el nivel de exposición a estos nanomateriales. Estos riesgos, junto con las medidas existentes de valoración de estos riesgos, ya han sido objeto de varios estudios[66], y, aunque estos materiales no son peligrosos por sí mismos, la conclusión general hasta ahora es que aún existe incertidumbre científica sobre la seguridad de estos nanomateriales en muchos aspectos y, por tanto, su valoración debe realizarse caso por caso.

Países como EE. UU., Australia, Canadá, Reino Unido y la Unión Europea[67][68] ya han empezado a recopilar información para entender estos riesgos potenciales y a revisar sus normativas para determinar posibles modificaciones.

Algunas de las aplicaciones civiles en la seguridad son:

- Detección de sustancias (químicas y biológicas), objetos y personas para prevenir problemas de seguridad[69]. Y se aplica en dispositivos de imágenes de rayos X, infrarrojos y teraherzios, sensores y redes de sensores para la detección de patógenos y químicos. El mayor avance es la posibilidad de redes autónomas de sensores que, además de capturar datos, procesen y transmitan la información y se comuniquen con otros sensores en entornos potencialmente hostiles. Dado el pequeño tamaño de estos dispositivos y su bajo precio, podrían convertirse en la siguiente generación de sensores. Además podrían reducir la intervención humana en lugares peligrosos.
- Protección (con equipos y filtros de descontaminación, y protección física).
- Identificación (incluida la lucha contra la falsificación y la autenticación, la medicina forense, la criptografía cuántica y el mercado de productos falsificados).

Los nanomateriales están empezando a usarse en aplicaciones de defensa, que buscan mejorar las herramientas disponibles para los soldados y la eficacia de los sistemas de armas. Determinados nanomateriales se usan como sensores en la detección de pequeñas trazas de explosivos que indican la presencia de

[66] Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR), http://ec.europa.eu/health/ph_risk/committees/04_scenihr/docs/scenihr_o_010.pdf
[67] La nanotecnología ha sido una prioridad clave de la Unión Europea tanto en el VI como en el VII Programa Marco a través de diversas iniciativas orientadas a aplicaciones de seguridad.
[68] En España el informe de 2008 de la Fundación Phantoms da una visión sobre el estado de la Nanociencia y Nanotecnología sobre las áreas temáticas siguientes: Energía, Nanobiología y Nanomedicina, Nanoelectrónica y Electrónica Molecular, Nanomateriales, Nanometrología, Nanoóptica y Nanofotónica, Nanotubos, Nanoquímica y Teoría, Modelado y Simulación.
[69] Detecta agentes biológicos, como virus, bacterias, ADN, ARN, proteínas, para prevenir el bioterrorismo, así como la diseminación biológica de algún agente peligroso (p. ej. ántrax, ébola); agentes químicos como venenos (gas sarín), gases industriales (p. ej. hidrógeno, monóxido de carbono); radiaciones: rayos alfa, beta y gamma; propiedades ópticas (longitud de onda e imágenes); otras propiedades físicas como la temperatura y presión.

minas. En el futuro, los nanomateriales pueden ayudar al desarrollo de nuevas aplicaciones y productos en un amplio espectro de defensa, como dispositivos de vigilancia, explosivos y uniformes militares.

Algunas aplicaciones duales (civil y militar) de la nanotecnología[70][71] son:

- Pilas de hidrógeno fabricadas con nanomateriales que podrían usarse en UAV (vehículos aéreos no tripulados), o como sistema secundario de energía.
- Materiales energéticos y combustibles avanzados con nanopartículas que alcanzan recubrimientos de mayor densidad y permiten la liberación de energía más rápida y eficiente. Su uso estaría orientado a combustibles o armas (pólvoras, explosivos).
- Comunicaciones seguras y criptografía cuántica mediante el empleo de emisores y receptores de fotones fabricados mediante nanotecnología, como los láseres modulados.
- Sensores sensibles en el rango visible y el infrarrojo que mejoran los sensores actuales de visión nocturna e infrarrojos.
- Invisibilidad: se consigue que la luz rodee una zona del espacio para que aparente atravesarla. Es aplicable en microondas (radar) y acústica (sonar). Se persigue conseguir en el futuro estos mismos fenómenos en longitudes de onda de visible e infrarrojos.
- Detección de agentes químicos y biológicos mediante nanosensores, que son nanotubos o nanohilos metálicos, que pueden absorber moléculas químicas. Tienen múltiples aplicaciones, como protección de infraestructuras críticas, etc.
- Microsistemas insectos espía, consistentes en una red de microsensores intercomunicados por radio o por comunicación óptica. Forman sistemas autónomos y de tamaño reducido y son fáciles de dispersar sobre un escenario amplio para recabar información.
- Combatiente del futuro, permite la equipación con elementos de peso reducido, para la generación y almacenamiento de energía, comunicaciones, nuevos tejidos para camuflaje y protección, sensores optrónicos y sensores NBQ.
- Nanomateriales para blindajes que tienen un peso reducido, proporcionan un blindaje más resistente aplicable a todo tipo de vehículos militares y con mayor capacidad de camuflaje.

Posibles riesgos

Como toda nueva tecnología, sus aplicaciones plantean desafíos y retos. Pero si se mira hacia la evolución humana no ha habido mejora de la civilización sin la tecnología, esta ha estado en la base.

[70] *Nanotechnology Highlights 2011*. IOP Publishing. Véase iopscience.org/nano
[71] *Technology and Innovation Futures. Technology Annex.* Foresight Horizon Scanning Centre. www.bis.gov.uk/foresight

Para poder disfrutar de los enormes beneficios de la nanotecnología, es imprescindible afrontar y resolver los riesgos. Para hacer esto, debemos primero comprenderlos, y luego desarrollar planes de acción para prevenirlos. La nanotecnología permitirá la fabricación y prototipos de una gran variedad de productos muy potentes. Es imprescindible estar preparados.

Aún se está investigando el impacto que la nanotecnología puede tener en la salud y en el medio ambiente**.**

Por ello, gobiernos[72] y científicos deberían acordar que los productos derivados de la nanotecnología no se comercialicen hasta que todos los efectos secundarios estén estudiados.

Algunos de estos riesgos son producto de una falta de normativa jurídica, y otros de demasiado control. Hará falta distintos tipos de legislación según cada campo específico. Una respuesta demasiada rígida o exagerada en estos sentidos podría dar lugar a la aparición de otros riesgos de naturaleza muy distinta, por lo que habrá que evitar la tentación de imponer soluciones aparentemente obvias a problemas aislados. Un único enfoque (comercial, militar, información libre) no podrá impedir todos los posibles riesgos de la nanotecnología.

Pero la nanotecnología también promete avances en otro campo no menos significativo: la industria armamentística, si bien los expertos no coinciden completamente respecto a lo que las evoluciones previsibles que la tecnología de lo más pequeño pueda aportar a los sistemas de defensa en las próximas décadas.

Algunos expertos comparan también las armas nanotecnológicas y las armas nucleares[73]. Ambos tipos de armas pueden estabilizar o desestabilizar la situación internacional, pero hay diferencias entre ellas. Así, por ejemplo, las armas nucleares causan destrucción masiva de forma indiscriminada; en cambio, las nanoarmas se podrían dirigir; se podrían fabricar de forma más rápida gracias al proceso de realizar prototipos, y su fabricación es más sencilla, mientras que las armas nucleares requieren un gran esfuerzo tanto de investigación como de fabricación. Por otra parte, mientras el transporte de armas nucleares antes de utilizarlas es difícil, con las nanoarmas sucede todo

[72] La Comisión Europea es consciente de la importancia que la nanotecnología tendrá en los próximos años y de lo lejos que está de las nuevas generaciones. Además, sabe que el debate que plantea el uso de nanotecnología es parecido al de los organismos transgénicos, con gente a favor o en contra, pero con pocas voces realmente expertas. Es por eso que ha creado el proyecto NanoChannels, con el que pretende informar y abrir el debate a la sociedad europea. www.nanochannels.eu También cuenta con el ECSIN-European Center for the Sustainable Impact of Nanotechnology, www.ecsin.it un centro internacional de investigación para caracterizar el impacto de las innovaciones de nanotecnologías en el entorno y en la salud, y para evaluar también los aspectos éticos y sociales.

[73] «Nanotechnology. Drexler and Smalley make the case for and against 'molecular assemblers'», *Chemical & Engineering News*, diciembre 1, 2003. See http://pubs.acs.org/cen/coverstory/8148/8148counterpoint.html

lo contrario. Por otra parte, se desconoce aún la capacidad de destrucción de las armas basadas en las nanotecnologías en comparación con la capacidad de destrucción de las armas nucleares. La gran diferencia respecto a estas armas convencionales es que las armas nanotecnológicas serán accesibles con mucha facilidad a pequeños países y grupos terroristas, ya que los materiales necesarios para su fabricación se podrán encontrar por todas partes, debido a los diversos y masivos usos civiles de las técnicas basadas en la nanotecnología.

Por tanto, el desarrollo de armas a través de la nanotecnología resulta más inseguro debido a diversas razones, como la mayor incertidumbre en cuanto a las capacidades del adversario, menor tiempo de respuesta a un ataque o mejor capacidad de dirigir la destrucción de los recursos del adversario.

Además, sin controles adecuados, el número de países con capacidad para desarrollar la nanotecnología podría ser mucho más alto que el número de países que tienen capacidad nuclear, químico o biológica. Y debido a ello, la nanotecnología podría desestabilizar las relaciones internacionales, reduciendo la influencia y la interdependencia económica, potenciando la capacidad de atacar objetivos específicos, como personas, pero también podría reducir la capacidad de un país de vigilar a sus enemigos potenciales o incluso eliminar la capacidad de los países más poderosos de controlar el escenario internacional.

Pero no solo existirían riesgos, sino que las nanotecnologías pueden también aportar grandes ventajas, como mejorar la capacidad defensiva de un país detectando con bastante tiempo a un posible agresor o disponiendo de armas de menor tamaño.

Otra ventaja teórica es que las nanotecnologías pueden aportar armas más limpias y seguras que causen menos daños colaterales que las convencionales, sin olvidar las capacidades experimentales de nanorobots espías. Sin embargo, la primera preocupación en lo que respecta al desarrollo de estas armas es la toxicidad, ya que productos que a niveles no moleculares no resultan tóxicos, permitidos incluso por los ministerios de sanidad en los alimentos, podrían ser enormemente tóxicos a nivel nanométrico[74].

INTELIGENCIA ARTIFICIAL APLICADA A VEHÍCULOS NO TRIPULADOS

Avances y posibles riesgos

Los vehículos no tripulados (UV, por sus siglas en inglés) responden a una extensa gama de misiones en todos los ámbitos tanto aéreos como submarinos, navales, terrestres, espaciales e incluso mixtos. El número de proyectos de sis-

[74] European Parliament, Science and Technology Options Assessment (STOA), *NanoSafety - Risk Governance of Manufactured Nanoparticles*, marzo 2012.

temas no tripulados ha crecido en los últimos dos años de manera exponencial y el desarrollo de cargas de pago, cada vez más sofisticadas, está alcanzando niveles desconocidos[75].

El empleo de los UAS, tanto en el campo militar como en el civil, está demostrando día a día grandes ventajas frente a las plataformas tripuladas en determinadas áreas de acción, especialmente en situaciones críticas o que presenten algún riesgo para el tripulante. Nadie duda ya de su eficacia, versatilidad y capacidades, previéndose un importante despliegue de sistemas aéreos no tripulados (UAS, por sus siglas en inglés) con un requisito de operación en toda la estructura del espacio aéreo, pero muchos son los retos todavía pendientes: la inserción en el espacio aéreo; la formación de los operadores; la certificación de aeronavegabilidad del sistema; los requisitos de espectro radioeléctrico para el mando y control y carga de pago, o la gestión de riesgos, entre otros muchos.

Misiones como guardacostas, vigilancia de fronteras, seguimiento agrícola, recogida de datos meteorológicos y/o atmosféricos, cartografía geológica de infraestructuras desde gran altitud, etc., son, entre otras actividades, las más significativas que estos aparatos desarrollarán en el ámbito civil en un futuro casi inmediato. En cuanto a las aplicaciones militares son igualmente numerosas, destacando la recolección de Inteligencia de señales e imágenes, vigilancia y reconocimiento (ISR, por sus siglas en inglés)[76], adquisición de objetivos, corrección de tiro, evaluación de daños, relé de comunicaciones, guerra electrónica, detección de dispositivos explosivos improvisados, misiones ofensivas, supresión de defensa aérea, y apoyo aéreo cercano.

El uso de los sistemas UAS en áreas de conflicto es cada día más intenso. También se están usando globos cautivos con fines militares. Por ejemplo, el uso de los llamados *drones* (vehículo aéreo no tripulado, UAV, por sus siglas en inglés) ha aumentado en los últimos años, armados o no con misiles. En concreto, la utilización de máquinas no tripuladas por parte de las Fuerzas Armadas de Estados Unidos y también de su Agencia Central de Inteligencia (CIA), ha seguido una tendencia creciente.

Estos robots ofrecen una serie de ventajas indiscutibles: son baratos en comparación con los medios tradicionales, más fiables, más rápidos, son ajenos a la fatiga, reducen los «daños colaterales», no conocen el miedo y, lo más importante, no arriesgan la vida del piloto. Estas características han provocado un gran interés hacia estas nuevas máquinas de guerra. En la actualidad, más de 40 países, entre los que se encuentra España, tienen acceso a la tecnología

[75] El accidente nuclear de Fukushima es la mejor muestra de lo que los vehículos no tripulados son capaces de hacer.

[76] Existe ya un nanoavión no tripulado de reconocimiento. Uno de los aviones no tripulados (UAV) más pequeños que cabe en la palma de la mano. Despega y aterriza como un helicóptero o se lanza manualmente. Para su control no necesita ordenadores personales y puede utilizar batería de sulfuro de litio.

asociada a estos robots y sus arsenales disponen en mayor o menor medida de algunos de ellos. Asimismo, al menos Israel y el Reino Unido han utilizado estos sistemas armados para atacar objetivos de «alto valor».

Los avances tecnológicos están permitiendo el desarrollo de una nueva generación de robots que estará lista antes de que finalice la década actual. El futuro en este campo pasa por la creciente automatización y la aparición de los denominados «robots autónomos letales» (RAL). El término «autónomo» debe entenderse en el sentido de que la máquina es capaz de adoptar por sí misma las decisiones necesarias sin ninguna participación humana, así como «aprender» de sus propias acciones.

La pugna para conseguir un arma que permita alcanzar a un enemigo a una distancia en la que él no pueda hacer lo mismo con el atacante es tan antigua como la guerra. Sin embargo, el empleo de UAV parece estar señalando un cambio esencial en los modos y formas en que hasta ahora se ha conducido la guerra, levantando importantes controversias.

Durante siglos, la aplicación de la fuerza letal en Occidente ha sido congruente con los principios del *ius ad bellum* (razones legítimas para entrar en guerra) y con el *ius in bello* (reglas aceptables en la guerra o Derecho Internacional Humanitario, DIH).

Sin embargo, las autoridades políticas pueden verse tentadas a iniciar una acción armada por medio de robots pudiendo incluso realizar una operación encubierta. Por consiguiente, la utilización de robots podría servir de incentivo para la acción armada, al eliminar los sentimientos éticos asociados a la guerra.

El empleo de esta nueva tecnología en el ámbito de un conflicto plantea nuevos interrogantes éticos y legales[77]que habrán de estudiarse y regularse. El uso de robots en los conflictos armados encierra un importante componente tecnológico, pero sin lugar a dudas son las cuestiones sociales, políticas y éticas las que comportarán una especial relevancia para el futuro. En cualquier caso, el debate sobre ética y guerra robotizada está ya sobre la mesa.

USO DUAL. INNOVACIÓN TECNOLÓGICA MILITAR

Relación estratégica con el sector civil

Desde una perspectiva histórica hay que situarse en los años posteriores a la Segunda Guerra Mundial, cuando se institucionalizan las políticas guberna-

[77] DIEEEO37-2011. *La utilización de drones en los conflictos actuales: una perspectiva del derecho internacional.* Pilar POZO SERRANO. Instituto Español de Estudios Estratégicos, mayo 2011.

mentales de I+D. Primero en EE. UU. y luego en Europa se inician los programas y planes de investigación científica y desarrollo tecnológico. Anteriormente, existía una estrecha conexión entre producción de sistemas militares y desarrollo tecnológico, aunque no se hacía de una manera sistematizada y planificada a largo plazo. No obstante, debe reconocerse la importancia de las políticas de defensa y de las tecnologías de los sistemas de armas en el nacimiento y consolidación del llamado «sistema de ciencia y tecnología»[78].

La importancia del desarrollo de la tecnología militar en la victoria de los aliados en la Segunda Guerra Mundial llevó a la preponderancia de esta tecnología sobre la civil, situación que continuó durante la Guerra Fría, que derivó en lo que se llamó «el complejo militar-industrial».

El final de la Guerra Fría, junto con otros factores, produjo un cambio paulatino en el que aumenta la importancia del desarrollo de tecnologías en el ámbito civil y el flujo de estas hacia las aplicaciones militares, dando lugar a lo que impropiamente se conoce como «tecnologías de uso dual», es decir, uso civil y uso militar. Hubo una fuerte disminución de los presupuestos de defensa en los países occidentales que obligó a buscar componentes y subsistemas de menor coste; además, cambió la percepción del concepto clásico de guerra mientras surgían nuevas amenazas a la seguridad nacional, como el terrorismo o los estados fallidos; de este modo, frente al concepto de «defensa», cobra importancia el nuevo concepto de «seguridad» en el que confluyen tareas propias de la seguridad doméstica o interior de los países con las de defensa militar, con fronteras muy poco definidas. Por otra parte, el desarrollo de muchas tecnologías en mercados civiles supera a los militares, como, por ejemplo, en el consumo de circuitos integrados.

Siguiendo esta tendencia, en 1992 la Unión Europea introduce en el Tratado de Maastrich la Política Exterior y de Seguridad Común (PESC), que daría lugar a la Política Europea de Seguridad y Defensa (PESD) y la creación, en 2004, de la Agencia Europea de Defensa (EDA), que entre sus funciones se encarga de la política de I+D+i para la defensa. Por otra parte, en el VII Programa Marco de la UE, de 2007, se incluye por primera vez una línea de «seguridad» para el ámbito civil, aunque en coordinación con la EDA. Se observa, no obstante, que en el ámbito político de la UE se mantiene la separación entre tecnologías para la defensa y tecnologías para la seguridad, pero la realidad muestra una fuerte confluencia entre ambas.

Por tanto, puede decirse que el sistema de innovación militar se ha vuelto más abierto, con sus ventajas e inconvenientes, y es objeto de estudio actualmente desde ambos sectores, el sector militar y el sector civil.

[78] El establecimiento de los sistemas de ciencia y tecnología procede del célebre informe de Vannevar BUSH *Science, the Endless Frontier*, de 1945, que planteaba un nuevo modelo de política científica, en el cual la I+D del sector militar jugaría un papel importante. Véase «La innovación en Seguridad y Defensa: aplicaciones duales de las tecnologías». *Cuadernos Cátedra* ISDEFE-UPM, julio 2011. http://catedraisdefe.etsit.upm.es

Sistema de innovación en la industria militar

Se están aplicando nuevos sistemas de innovación en las industrias del sector de la defensa. El sistema de innovación militar se enfrenta a un proceso de cambio debido a procesos interdependientes, que nos lleva a un sistema más abierto respecto a los años 40 a 80 (Guerra Fría), con fronteras poco definidas pero con la permanencia de características del sistema anterior.

Durante este período de la Guerra Fría los sistemas eran competitivos, complejos, con altas prestaciones, pero altos costes; las industrias eran intensivas en conocimiento. Era un sistema de innovación cerrado: las empresas estaban altamente especializadas, había una red claramente definida y estable de laboratorios especializados, las relaciones eran estrechas entre empresas, laboratorios y el cliente militar, y existía una clara influencia del cliente en la definición del sistema; este sistema de innovación se diferenciaba de las industrias civiles en sus costes y complejidad creciente, basados en una «cultura» diferente y series de producción cada vez más cortas.

Hay que reconocer el papel de la industria militar en la raíz de muchas innovaciones y en el desarrollo de tecnologías de uso genérico. Hasta ahora nos basábamos en que los ámbitos civil y militar son claramente diferentes, sin embargo, los cambios tecnológicos, estratégicos e institucionales cuestionan esta afirmación. Existe un claro trasvase de tecnologías en ambas direcciones que beneficia a los dos ámbitos.

El primer proceso de cambio que afecta al sistema de innovación militar es el cambio tecnológico. Se pasa de un modelo de acumulación tecnológica vertical a un modelo horizontal, emergen nuevas tecnologías horizontales (nanotecnología, biotecnología, etc.) que presentan nuevas oportunidades y desafíos para el futuro de la defensa y la seguridad. Las tecnologías de origen civil pasan a dominar (en volumen de mercado y en prestaciones) amplias áreas relevantes para la defensa (electrónica, telecomunicaciones, etc.) al tiempo que se reduce su coste.

Un segundo proceso es la organización de la producción. Surgen nuevas estrategias de organización de la producción, como la externalización de la misma e incluso de la I+D, surgen redes complejas de proveedores, PYMES orientadas a varios clientes, etc. Se da una reestructuración industrial: los clientes abandonan tareas como el mantenimiento, la gestión de bienes inmuebles, incluso la financiación y pasan de ser compradores de sistemas a ser compradores de servicios. Esto implica que los proveedores tradicionales necesitan desarrollar nuevas competencias al tiempo que entran otros nuevos proveedores de servicio. Esta nueva organización afecta también a los OPI u organismos públicos de investigación de defensa que históricamente habían estado separados

por cuestiones de seguridad y mantenían relaciones estrechas con defensa y fuerzas armadas; actualmente buscan adquirir conocimientos relevantes en campos científicos y tecnológicos más amplios, acceder a tecnologías y capacidades «civiles», expandir su presencia en el campo de la seguridad y aplicar tecnologías militares a usos civiles; para ello necesitan más flexibilidad en sus estrategias de comercialización y privatización, y aplicar estrategias más abiertas y con un nivel de especialización decreciente.

El tercer proceso se refiere a la estructura de los mercados. Se da una convergencia entre la defensa y la seguridad. Se ha ampliado el papel de las agencias de seguridad, así como la definición de seguridad. Ahora las fuerzas militares participan en tareas de seguridad, policiales, pero también en la recuperación ante desastres naturales (Unidad Militar de Emergencias), problemas de inmigración (como sucede con el Department de Homeland Security de EE. UU. o el europeo «Security Research Programme») o cuestiones de «Seguridad Humana». La separación entre defensa militar y seguridad nacional se difumina; así, los proveedores militares penetran los mercados de seguridad y surgen nuevos grupos de investigación en el campo de la seguridad (expertos en infraestructuras, etc.).

En el contexto europeo, el mercado europeo de defensa está fragmentado. Aún no están integradas las actividades de defensa (incluidas industria e investigación) en el ámbito de la UE, pero las nuevas políticas de seguridad y defensa buscan ese objetivo, un ejemplo de ello es que la I+D en el campo de la seguridad es ya parte del Programa Marco. Por parte de la Comisión Europea, en 2010 presentó la iniciativa «Unión por la Innovación», como pieza clave de su Estrategia 2020 como marco de trabajo de la UE.

En este nuevo sistema abierto de innovación militar habría que redefinir las funciones institucionales, de modo que se amplíe el concepto de seguridad y se produzca una convergencia de misiones. En este contexto emergen nuevos mercados muy cercanos (agencias y programas de seguridad) con nuevos proveedores de aplicaciones militares, sin olvidar la importancia de las tecnologías de origen civil que también proporcionan nuevos proveedores e impulsarán la diversificación de los OPI de defensa.

Política de I+D+i en el sector de la Defensa Española

La política de innovación en España comenzó a desarrollarse de manera sistemática y sostenida a partir de la llamada «Ley de la Ciencia de 1986» o Ley de Fomento y Coordinación General de la Investigación Científica y Técnica cuyo instrumento fueron los Planes Nacionales de I+D.

Uno de los objetivos de interés general de la ley era: «El fortalecimiento de la defensa nacional». Además establecía que: «El Ministerio de Defensa podrá

adaptar el Plan Nacional y, en su caso, integrar en él proyectos de investigación científica y desarrollo tecnológico en materias que afecten a la defensa nacional, para su financiación, en todo o en parte con cargo a dicho Plan, así como financiar proyectos integrados en los mismos».

Desde entonces, se ha ido integrando la I+D de carácter militar en las políticas generales. Hasta el año 2004 los Planes Nacionales incluían en su función de gasto presupuestario el «Sector de la Defensa», que pasaría luego a ser de la «Defensa y la Seguridad» siguiendo las tendencias descritas anteriormente.

Todo esto tiene su continuación en la nueva Ley de la Ciencia, la Tecnología y la Innovación de 2011[79].

En la nueva Ley de la Ciencia de 2011 se señala la importancia de coordinar las políticas de investigación científica y técnica en la Administración General del Estado y favorecer la internacionalización, especialmente en el ámbito de la Unión Europea. En base a ello se considera conveniente designar un interlocutor único en el seno de este Departamento de Defensa.

En el caso de la defensa española, en 2010 se presentó la Estrategia de Tecnología e Innovación para la Defensa, ETID, que se integra dentro de esta ley. La ETID difunde de manera abierta cuáles son las tecnologías prioritarias para nuestras Fuerzas Armadas, así se hace posible que las empresas del sector de defensa puedan orientar sus actividades en I+D hacia dichas tecnologías, optimizando su esfuerzo inversor. Con esta filosofía, el programa COINCIDENTE[80] constituye un vehículo para favorecer la incorporación de tecnologías desarrolladas dentro del ámbito civil a aplicaciones de defensa. Se abren así los avances en el campo civil hacia el mercado de defensa, mejorando la competitividad de los productos y servicios al actuar como mecanismo multiplicador de las inversiones ya realizadas anteriormente. Los proyectos desarrollados en el marco de este programa contribuyen a fomentar el tejido industrial, científico y tecnológico dedicado a la defensa.

Continuando con este objetivo, la Orden DEF/685 de 2012 (BOE n.º *82, 5-4-2012), regula y coordina la investigación y desarrollo de sistemas de armas y equipos de interés para la defensa nacional en el ámbito del Ministerio de Defensa.*

[79] Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, establece el marco para el fomento de la investigación científica y técnica y sus instrumentos de coordinación general. Su objetivo es promocionar la investigación, el desarrollo experimental y la innovación como elementos sobre los que ha de asentarse el desarrollo económico. Véase en www.boe.es/boe/dias/2011/06/02/pdfs/BOE-A-2011-9617.pdf

[80] COINCIDENTE, Programa de Cooperación en Investigación Científica y Desarrollo en Tecnologías Estratégicas. Está dentro del programa nacional de I+D como fomento del tejido industrial en I+D respecto a Defensa.

La Dirección General de Armamento y Material (DGAM), dependiente de la Secretaría de Estado de Defensa (SEDEF), se configura como interlocutor único en cuanto a las citadas actividades de I+D de Defensa.

La DGAM, para la elaboración de la política de I+D, cuenta con el asesoramiento del Sistema de Observación y Prospectiva Tecnológica (SOPT[81]) de la Subdirección General de Tecnología e Innovación (SDGTECIN), así como del Instituto Nacional de Técnica Aeroespacial Esteban Terradas (INTA), en materia aeroespacial.

Los organismos autónomos adscritos al Ministerio de Defensa, Instituto Nacional de Técnica Aeroespacial (INTA) y Canal de Experiencias Hidrodinámicas de El Pardo (CEHIPAR), junto con el Instituto Tecnológico La Marañosa (ITM), suponen un gran impulso a las actividades de I+D en este ministerio.

CONCLUSIONES

El peligro tecnológico es uno de los potenciadores o multiplicadores de riesgo señalados por la Estrategia Española de Seguridad que puede materializarse en el nuevo ámbito del ciberespacio, como en los otros cinco considerados, los tradicionales tierra, mar, aire y espacio, más el informativo.

Las nuevas tecnologías de la información y la comunicación, junto a tecnologías que se apoyan transversalmente en otras, como son la nanotecnología, la biotecnología, la inteligencia artificial, amén de otras no consideradas en la EES, como la neurociencia, la ciencia cognoscitiva, etc., albergan en sus aplicaciones nuevas y crecientes fuentes de progreso generadores de bienestar y riqueza.

El avance tecnológico, que permite a la humanidad progresar, ofrece múltiples y variadas facetas según su uso e intención de uso: es factor de competitividad, plantea problemas de seguridad, puede ser potenciador y minorador de riesgos, la dualidad de su uso civil y militar…

Al mismo tiempo, la mayor dependencia de la tecnología nos hace también más vulnerables. Las nuevas funcionalidades facilitan la vida diaria, pero también vienen acompañadas por vulnerabilidades tradicionales y otras nuevas que afectan a nuestra seguridad, ya sea como ciudadanos, empresas o como estados.

Diversos actores, como activistas políticos, grupos terroristas, delincuencia organizada, estados enemigos o individuos aislados pueden ser agentes a los que el

[81] Más información en el Portal de tecnología e Innovación del Ministerio de Defensa. Véase www.tecnologiaeinnovacion.defensa.gob.es/es-es/Paginas/Inicio.aspx

empleo de la tecnología les facilita la comisión de sus ataques, cuyos objetivos son variados: infraestructuras críticas, conocimiento industrial y tecnológico, sistemas financiero y económico, datos personales de ciudadanos, etc.

Sobre la tecnología habrá que mantener una intensa y constante vigilancia para detectar no solo las nuevas y posibles mejoras y avances, sino los efectos colaterales sobre otros aspectos, como la seguridad nacional, la seguridad personal, los dilemas éticos y la falta de regulación. La tecnología debería enmarcarse siempre en un contexto de seguridad que no multiplique o genere nuevas amenazas y riesgos.

La innovación tecnológica militar se ha visto superada por la innovación en el ámbito civil, algunas de cuyas aplicaciones son susceptibles de ser incorporadas al ámbito militar. Además de conservar esta relación que supone un intercambio de aplicaciones innovadoras, es necesario impulsar y coordinar una estrategia de colaboración entre ambos sectores que contribuya a la seguridad nacional, amén de contribuir a mejorar el nivel de innovación y competitividad.

Es por ello que la EES aboga por un enfoque integral de las diversas dimensiones de la seguridad.

En aplicación de lo recogido en la Estrategia, entre las directrices de la Directiva de Defensa Nacional de 31 de julio de 2012 se subraya el empleo de la disuasión creíble y suficiente ante posibles amenazas, así como la reacción a las agresiones. Respecto a la disuasión «se participará en el impulso de una gestión integral de la ciberseguridad», una de las iniciativas planteadas en la EES para contrarrestar las ciberamenazas, «en el marco de los principios que se establezcan al efecto en la futura estrategia de ciberseguridad», una de las estrategias de segundo nivel apuntadas por la EES. En este enfoque integral «deberían participar los centros de alerta temprana nacionales junto con los sectores de telecomunicaciones y los proveedores de servicios de telecomunicaciones».