DOCUMENTO DE TRABAJO 12/2015

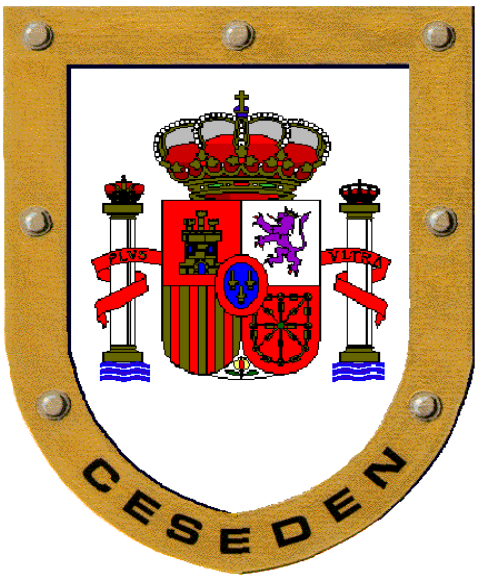
PLAN ANUAL DE INVESTIGACIÓN 2015

ORGANISMO SOLICITANTE DEL ESTUDIO:

CESEDEN

TECNOLOGÍAS DISRUPTIVAS Y SUS EFECTOS SOBRE LA SEGURIDAD

TECNOLOGÍAS DISRUPTIVAS Y SUS EFECTOS SOBRE LA SEGURIDAD



Mayo 2015

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL (CESEDEN)

ÍNDICE

INTRODUCCIÓN

Jordi Marsal
Adjunto civil al Director del CESEDEN

Uno de los elementos que definen una cultura estratégica es el papel que juega la tecnología en su forma de hacer la guerra. Unas culturas, como la norteamericana, expresan una preferencia radical por la tecnología como factor que define su superioridad para obtener la victoria en la confrontación.

Los factores tecnológicos, humanos y doctrinales, y su desarrollo equilibrado permiten la operatividad eficaz de unas Fuerzas Armadas. Los cambios tecnológicos tienen una incidencia fundamental en los cambios sociales, tanto los civiles como los militares. Estos cambios en las tecnologías acostumbran a desarrollarse paulatinamente, pero a veces la aparición de algunas nuevas tecnologías o un nuevo uso de alguna ya existente, suponen un cambio radical en el mundo científico, en el conjunto de la sociedad y en la forma de enfrentarse a los conflictos.[1] Nos hallamos ante revoluciones científico-tecnológicas en general y auténticas revoluciones en el ámbito militar. Así, por ejemplo, en las dos últimas décadas del siglo pasado, el desarrollo de las tecnologías de la información y sus aplicaciones unido a la aparición de las armas de precisión, dio lugar a la llamada Revolución en Asuntos Militares (RMA, en sus siglas inglesas)[2] que fué también punto de partida en los llamados procesos de Transformación de las Fuerzas Armadas, que ha comportado profundos cambios en las doctrinas y estrategias, en la organización y el funcionamiento tanto de las Fuerzas Armadas como en el conjunto de las políticas de seguridad y defensa.

Estas revoluciones tienen un carácter disruptivo, a las tecnologías que las producen las llamamos disruptivas: "una tecnología disruptiva es aquella que convierta en obsoleta una tecnología existente, cambiando desde la forma de operar hasta incluso el propio tejido industrial".[3] También puede suceder que se produzca un nuevo enfoque en el uso de una tecnología ya existente, así "una disrupción implica utilizar un enfoque radicalmente diferente a la hora de abordar un problema de forma que se obtenga una ventaja competitiva".[4]

1 La bibliografía sobre las relaciones entre sociedad, tecnología y guerra es amplia. Una obra reciente que resume de forma didáctica y profunda la historia de estas relaciones es JUAN CARLOS LOSADA (2014): De la honda a los drones. La guerra como motor de la historia. Barcelona, Pasado y Presente.

2 Uno de los mejores estudios sobre este tema publicados en España es GUILLEM COLOM (2008): Entre Ares y Atenea. El debate sobre la revolución en asuntos militares. Madrid, IUGM.

3 PATRICIA LÓPEZ VICENTE (2009): Tecnologías Disruptivas. Mirando el futuro Tecnológico. En Boletín de Observación Tecnológica en Defensa nº 25, pp 16-19.

4 Ibídem.

En el ámbito militar la aplicación de tecnologías disruptivas produce, si se quiere obtener una superioridad en el enfrentamiento, cambios operativos con sus consecuencias organizativas y con ello cambios doctrinales y estratégicos profundos que tendrán también un carácter disruptivo.

La historia está llena de ejemplos: el uso del caballo con los carros de combate o la aparición de la caballería en la antigüedad; el uso de la pólvora tanto en el armamento de mano como en la artillería durante el paso de la Edad Media al Renacimiento; la aviación, el submarino[5] o la energía nuclear y la creación de las armas nucleares ya en el siglo XX. Son algunos ejemplos históricos que reflejan los profundos cambios que se produjeron en el Arte de la Guerra con sus consecuencias operativas, orgánicas, doctrinales y estratégicas.

La innovación es fundamental para la evolución y el progreso de la sociedad. Las organizaciones que se cierran al cambio están condenadas a desaparecer ante aquellas que introducen innovaciones en los distintos campos de actividad social. Las organizaciones, especialmente cuanto más complejas son, mantienen fuertes resistencias a cambiar para adaptarse a los nuevos retos y entornos. Por ello los esfuerzos e inversiones (tanto intelectuales como materiales) para fomentar la innovación son fundamentales para triunfar en los nuevos escenarios. Y así es también en el campo de la seguridad y de la defensa, y concretamente en lo militar.[6]

Estos cambios tienen sus consecuencias también en los campos legales y éticos.[7] La nuevas formas de afrontar los conflictos pueden convertir en obsoletos los sistemas jurídicos que regulaban la confrontación al no dar respuestas adecuadas a nuevas situaciones que pueden darse. La aparición y el uso de estas tecnologías plantean problemas y debates éticos, a veces de gran intensidad, sobre su aplicación y las

5 Los escenarios submarinos y la aplicación de nuevas tecnologías tanto de uso defensivo como ofensivo y en el marco de las estrategias A2/AD y las correspondientes contraestrategias parece que volverán a jugar un papel importante en las próximas décadas. Véase BRYAN CLARK (2015): The Emerging Era in Undersea Warfare. Washington, Center for Strategic and Budgeting Assessment.

6 El profesor Javier Jordán ha reflexionado profundamente sobre estos aspectos y así ha publicado una serie de interesantes documentos en el GESI (Grupo de Estudios de Seguridad Internacional) de Granada:

-"Una introducción al concepto de innovación militar", análisis GESI nº 6/2014,

-"Fases de la innovación militar. La Batalla Aeroterrestre como caso de estudio", análisis GESI nº7/2014,

-"Innovación y Revolución en los asuntos Militares: una perspectiva no convencional", análisis GESI 10/2014,

-"¿Qué factores impulsan la innovación militar?", análisis GESI nº12/2014,

-"El cambio doctrinal, clave de la innovación militar", análisis GESI nº 15/2014.

7 Por ejemplo el Center for a New American Security ha abierto un "Ethical Autonomy Project" http://www.cnas.org/ethicalautonomy.

posibles consecuencias. Pensemos en debates que se produjeron con la aparición del arma submarina o el posible uso e incluso existencia de las armas nucleares. Hoy se ha abierto un debate sobre el uso de robots,[8] especialmente si se consigue un tal grado de autonomía frente al control humano.[9] Mientras estamos redactando los textos finales de esta publicación se está realizando una conferencia en Ginebra en el marco de NNUU a partir de un documento elaborado por Human Rights Watch[10] para plantear la posibilidad de prohibir el uso de armas robóticas totalmente autónomas.[11] También los debates sobre el uso de UAV's con armamento de precisión en la lucha antiterrorista por sus implicaciones legales y éticas en procedimientos de ejecución de líderes terroristas y los posibles "daños colaterales" que pueden producirse y se producen.[12] Tampoco debemos olvidar los debates sobre el uso de armas cibernéticas en el ciberespacio ante la difícil atribución del ataque recibido. Estos debates pueden incluso tener implicaciones lingüísticas: el paso del uso de UAV (Unmanned Aerial Vehicle- Vehículo Aéreo no tripulado) al de RPAS (Remotely Piloted Aircraft System- Sistema Aéreo Pilotado Remotamente) tiene significativas implicaciones semánticas ante los debates que se realizan sobre estos temas.

Hablar de tecnología, de innovación tecnológica, es más amplio que un debate puramente tecnológico, aunque sin un profundo conocimiento de las tecnologías los demás debates pueden llegar a ser inadecuados o incluso surrealistas en algunos casos.

En el marco del CESEDEN desde hace tiempo funciona un grupo asesor sobre cuestiones tecnológicas y son diversas las publicaciones, tanto de EALEDE como del IEEE, que han tratado en profundidad diversas tecnologías y sus aplicaciones.

Así en Monografías del CESEDEN se ha publicado:

- VVAA (2012): El ciberespacio. Nuevo espacio de confrontación. (nº 126)
- VVAA (2012): Los ámbitos no terrestres en la guerra futura. Espacio. (nº 128)
- VVAA (2013): Necesidad de una conciencia nacional de Cibereseguridad. La Ciberdefensa un reto prioritario. (nº 137)

8 MICHAEL HOROWITZ and PAUL SCHARRE (2015): Meaningful Human Control in Weapons Systems. Washington, Center for a New American Security.

9 ALEX LEVERINGHAUS and GILLES GIACCA (2014): Robo Wars. The regulation of Robotic Weapons. Oxford Martin School

10 Mind The gap. The lack of Accountability for Killer Robots (2015). Washington, HRW.

11 Durante su desarrollo la prensa se ha hecho eco de estos debates (a veces en forma muy efectista). Así puede verse en artículos como "Los 'robots asesinos' salen de la ciencia-ficción" (EL PAÍS, jueves 9 de Abril de 2015, p7) o "El desafío de los robots asesinos" (EL MUNDO, 14 de abril de 2015 pp17-19).

12 ANTHONY DWORKIN (2013): Drones and targeted killing. Defining a European position. Londres, European Council on Foreign Relations.

- VVAA (2014): Nanociencia, nanotecnología y defensa (nº 142).
- En Documentos de Seguridad y Defensa han sido:
- VVAA (2011): Tecnologías del espacio aplicadas a la Industria y Servicios de la Defensa. (nº 41)
- VVAA (2012): Los sistemas no tripulados. (nº 47)
- VVAA (2012): Tecnologías asociadas a sistemas de enjambres de microUAV. (nº 49)
- VVAA (2014): Estrategia de la información y seguridad en el ciberespacio. (nº 60)
- VVAA (2014): El impacto de las nuevas tecnologías y las formas de hacer la guerra en el diseño de las Fuerzas Armadas. (nº 61)
- Y en los Cuadernos de Estrategia del IEEE:
- VVAA (2010): Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. (nº 149)
- VVAA (2011): Proliferación de Armas de Destrucción Masiva y de tecnología avanzada. (nº 153)
- VVAA (2011): La defensa del futuro: innovación, tecnología e industria. (nº154)
- VVAA (2014): El sector espacial en España. Evolución y perspectivas. (nº 170)

El IEEE también ha publicado un Documento de Investigación sobre biomímesis[13]

Decíamos antes que la cultura estratégica norteamericana se basa en conseguir la superioridad tecnológica frente a sus adversarios. En estos momentos existe en este país una percepción de que la superioridad tecnológica que han mostrado hasta el momento está en peligro ya que las tecnologías en que se basaba su superioridad están ya al alcance de otros actores o lo estarán en breve espacio de tiempo.

Esta superioridad durante la segunda mitad del siglo XX se basó desde el final de la Segunda Guerra Mundial en la tecnología atómica y a partir de los años 80 en las tecnologías de la información y en las tecnologías del armamento de precisión. La percepción de la posible pérdida de superioridad tecnológica conduce a la necesidad de plantearse una nueva fase de revolución militar basada en nuevas tecnologías disruptivas o en la utilización disruptiva de algunas existentes.[14]

13 VVAA (2014): Biomímesis en los entornos de Defensa y Seguridad. Madrid, IEEE Documento de Investigación 04/2014.

14 Véanse los excelentes informes realizados por LUÍS SIMÓN (2015): Offset strategy: ¿hacia un

Así el 15 de noviembre de 2014 el aún Secretario de Defensa, Chuck Hagel, lanzó la llamada "Defense Innovation Initiative".[15] Esta iniciativa además de plantearse la necesidad de importantes cambios en la organización del Pentágono y en la profundización de los procedimientos de adquisiciones,[16] se centra en la llamada "Third Offset Strategy" que tiene como finalidad una nueva disrupción tecnológica que permita a los EEUU mantener su amplia superioridad militar frente a cualquier posible competidor de acuerdo con los documentos doctrinales y estratégicos vigentes en este país. Este proceso que se abre cuenta con la colaboración de varios think tanks (especialmente el Center for Strategic and Budgetary Assessments[17] y el Center for a New American Security)[18] que han elaborado ya diversos documentos.

Las tecnologías prioritarias que se apuntan en un proceso que tan sólo acaba de empezar están relacionadas con la robótica y los vehículos autónomos, las armas de energía dirigida, el enfrentamiento submarino, etc.

Evidentemente la apertura de este proceso puede aumentar aún más el gap tecnológico entre los EEUU y los países europeos, con las consiguientes consecuencias sobre la falta de interoperabilidad entre sus respectivas Fuerzas Armadas o el desarrollo de sus Bases Tecnológicas e Industriales para la Defensa. Esta posibilidad no deja de preocupar a los propios norteamericanos, así como a países europeos, de forma que algunos de ellos ya han enviado a grupos para seguir este proceso. Si se crea un ambiente de colaboración será ventajoso para ambas orillas del Atlántico.

La experiencia ya existente en el campo de las organizaciones internacionales como la OTAN, la EDA o la LoI debe permitir el desarrollo y aplicación de estas innovaciones para mantener un suficiente grado de compatibilidad entre los sistemas de armas y las doctrinas entre todos los aliados occidentales.

Para España debe ser también importante no quedarse al margen de estos procesos y, salvando todas las distancias de recursos e intereses geopolíticos, no sería conveniente ni para nuestra política de seguridad y defensa ni para nuestro tejido industrial, tanto

---

nuevo paradigma de defensa en EEUU? Madrid, Real Instituto Elcano, ARI 14/2015; y por GUILLEM COLOM (2015): Washington, ¡tenemos un problema! ¿Cómo mantener la supremacía militar del país en un entorno cambiante? Madrid, IEEE Documento de Opinión 21/2015.

15 Office of the Secretary of Defense (OSO): The Defense Innovation Initiative (15 de noviembre de 2014).

16 ANDREW PHILIP HUNTER AND DENISE ZHENG (2015): Better Buying Power 3.DOD's New Plan for Technical Excellence and Innovation. Washington, Center for Strategic and International Studies.

17 ROBERT MARTINAGE (2014): Toward a New Offset Strategy. Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability. Washington, CSBA.

18 Este centro de Washington desarrolla un amplio programa de investigación y publicaciones bajo el nombre de "Beyond Offset". http://www.cnas.org/beyondoffset .

el militar como el civil. El Observatorio Tecnológico de la DGAM[19] debe jugar, a partir de su ya consolidada experiencia, un papel central para detectar y analizar la evolución que se produce en el desarrollo tecnológico, la detección de tecnologías disruptivas y sus posibles consecuencias. A partir de ello tanto el Ministerio de Defensa como aquellos que tienen relación con las industrias, la tecnología o la innovación, de forma coordinada deben implementar políticas que aprovechen las ventajas competitivas de la utilización de estas tecnologías.

En setiembre del año 2014 el Center for Technology and National Security Policy (CTNSP) de la National Defense University (NDU) publicó un estudio[20] en que analizaba las diferentes áreas donde se estaban y se iban a desarrollar nuevas tecnologías disruptivas. Tales áreas eran:

- El campo de las telecomunicaciones y el ciberespacio.
- El campo de la energía.
- El campo de los sistemas militares autónomos y no tripulados.
- El campo de las armas de energía dirigida.
- El campo de la biotecnología.

Y en una serie de anexos identificaba las tecnologías clave emergentes, así en:

- La biología, la biotecnología y la medicina.
- La robótica, la inteligencia artificial y el aumento de las capacidades humanas.
- Las telecomunicaciones y la ciencia cognitiva.
- La nanotecnología y los materiales avanzados.
- La energía.

Este trabajo no pretende ser una enciclopedia sobre el tema ni abarcar todas las áreas, sino plantear algunos análisis y cuestiones que son de interés en estos momentos desde una perspectiva española. Aunque en cada capítulo se tratan tecnologías específicas en función de sus consecuencias en cada perspectiva, nos pareció interesante centrarse especialmente en algunas áreas y algunas tecnologías. Así escogimos el campo de

19 Se puede acceder a él y a sus publicaciones a través del Portal de Tecnología e Innovación del Ministerio de Defensa (http://www.tecnologiaeinnovacion.defensa.gob.es). También puede encontrarse una historia de sus 10 años de existencia en DGAM: 10 años de Boletín de Observación Tecnológica de la Defensa (2014). Monografía del SOPT nº 14.

20 JAMES KADEKE and LINTON WELLS III: Policy Challenges of Accelerating Technological Change. Security Policy and Strategy Implications of Parallel Scientific Revolutions. Washington, CTNSP at NDU, DTP 106.

la robótica y los artefactos autónomos, el campo de la energía y concretamente las armas de energía dirigida y las tecnologías que permitan una mayor autonomía en los despliegues, el campo de las nanotecnologías y especialmente el grafeno-. Sin olvidar cuestiones relacionadas con el ciberespacio.[21]

El cuaderno se divide en tres capítulos. El primero se centra en un análisis de estas tecnologías; el segundo en las consecuencias operativas, doctrinales y estratégicas para las Fuerzas Armadas; y el tercero en las consecuencias y los debates alrededor de los aspectos legales y éticos. Finalmente se presentan unas conclusiones y recomendaciones que hagan de este trabajo no únicamente un esfuerzo teórico sino que puedan aportar algunos aspectos prácticos de utilidad para el presente con perspectivas de futuro.

Los autores fueron seleccionados pensando en la riqueza que supone el enfoque desde distintas perspectivas y experiencias. Así hemos unido tres perspectivas diferentes. La experiencia de la Dirección General de Armamento y Material (DGAM) y especialmente de su Observatorio Tecnológico; la experiencia del trabajo de reflexión y enseñanza de la Escuela Superior de las Fuerzas Armadas (ESFAS) del CESEDEN; y la experiencia de la actividad privada con la práctica jurídica relacionada con la tecnología y las empresas.

En el primer capítulo el Capitán de Fragata José María Riola, de la Subdirección de Planificación, Tecnología e Innovación de la DGAM, nos presenta la dimensión tecnológica de la innovación disruptiva en el ámbito de la defensa. En primer lugar expone la importancia de las tecnologías disruptivas en Defensa para, a continuación, centrarse en las cuestiones de qué es una tecnología con potencial disruptivo y su identificación y su análisis, señalando la importancia de la prospectiva como una herramienta de base para tal identificación. Introduce las experiencias ya existentes tanto en el ámbito del Ministerio de Defensa como en organizaciones internacionales como la LoI, la OTAN y la EDA. Tras estos aspectos previos entra ya en el análisis de la situación actual y las perspectivas de futuro de algunas áreas: las armas de energía dirigida mediante láser de alta potencia; los sistemas autónomos, la robótica y la biomímesis; la nanotecnología; y la generación y almacenamiento de energía en campamentos y armas.

En el segundo capítulo el Coronel José Luis Cabello Rodríguez, de la Escuela Superior de las Fuerzas Armadas del CESEDEN, nos habla del impacto operativo, doctrinal y estratégico de la aplicación de tecnologías disruptivas en la seguridad y la defensa. Expone, en primer lugar, unas reflexiones históricas sobre el tema y se centra

21 En los últimos tiempos son innumerables los escritos sobre cuestiones relacionadas con las actividades en el ciberespacio y aspectos relativos a la defensa y al ataque en el ciberespacio. Señalamos dos de los últimos documentos sobre los aspectos legales: MICHAEL N. SCHMITT (2015): The Law of Cyber Targeting. CCDCOE, Tallin Paper nº 7; y JESÚS REGUERA (2015): Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario. Granada, GESI análisis nº 7.

con mayor extensión y profundidad en las consecuencias de las armas nucleares. Así analiza sus consecuencias operacionales, tácticas y estratégicas. Entra, a continuación, en diversas consideraciones sobre algunas disrupciones que en el pasado y en el presente tiene la aplicación de estas tecnologías y en una perspectiva de futuro algunas consecuencias que pueden producirse con el desarrollo de la nueva "Third Offset Strategy" norteamericana. Desarrolla aspectos relacionados con la relación entre hombre y máquina en el campo de batalla en el marco de la progresiva autonomía de ésta respecto a aquel. En este marco analiza a fondo cuestiones relacionadas con el incremento del uso de los UAV's. También reflexiona sobre algunas consecuencias del uso de sistemas autónomos sobre la Seguridad Nacional, exterior e interior, y en las opiniones públicas.

Desarrolla, a continuación, los aspectos relacionados con los sistemas de energía proyectable, las aplicaciones militares del grafeno y las armas de energía dirigida. Finalmente extrae algunas conclusiones de las experiencias de las consecuencias que ha tenido la búsqueda de la superioridad a través del uso de las tecnologías disruptivas.

En el tercer capítulo la abogada Ana Marzo Portera desarrolla aspectos relacionados con las consecuencias legales y éticas que surgen a partir de la aplicación de tales tecnologías, especialmente algunas de ellas relacionadas con los profundos cambios en el campo de las comunicaciones y de los sistemas autónomos. Así tras una introducción sobre aspectos legales en el campo internacional y el europeo nos adentra en el mundo del ciberespacio en sus aspectos de ciberdelincuencia, ciberterrorismo y ciberguerras. Analiza diversos aspectos desde las perspectivas europeas y españolas para centrarse a continuación en el tratamiento de la información y su marco jurídico en relación con la confidencialidad y las cuestiones relacionadas con la propiedad intelectual. Finalmente analiza algunas consecuencias y problemas legales y éticos consecuencia de la aplicación de tecnologías que permiten el uso de robots, sistemas autónomos y armas inteligentes.

A partir de estos estudios y de los debates mantenidos a lo largo del trabajo se formulan una serie de conclusiones generales y recomendaciones desde una perspectiva general y también de su incidencia para España.

Para dar coherencia y continuidad a estos trabajos ha sido fundamental el trabajo del Coronel José Tomás Hidalgo Tarrero de la Escuela de Altos estudios de la Defensa (EALEDE) del CESEDEN como secretario del grupo de trabajo.

CAPÍTULO 1

LA DIMENSIÓN TECNOLÓGICA DE LA INNOVACIÓN DISRUPTIVA EN EL ÁMBITO DE DEFENSA

C.F. Ingeniero José María Riola Rodríguez
SDG PLATIN - DGAM

Resumen

La tecnología es un factor de indiscutible poder transformacional de la sociedad que se ha puesto de manifiesto desde los orígenes del hombre, pero su efecto disruptor ha sido incluso capaz de dar vuelcos radicales a los modelos económicos, sociales, políticos y éticos. El sector de la Defensa, punta de lanza históricamente del desarrollo tecnológico, es un claro ejemplo de ello, ya que hallazgos tecnológicos con un alto grado de disruptividad han conseguido en multitud de ocasiones cambiar las estructuras de poder y el orden mundial.

La mayoría de las naciones, conscientes del efecto diferenciador de la tecnología, invierten en mayor o menor grado en el ejercicio de predecir los cambios tecnológicos que vendrán en el futuro, su impacto, coste y beneficios, de manera que puedan explotar oportunidades y mitigar riesgos inherentes a la adopción o no de hallazgos tecnológicos.

En este capítulo, se pretende dar las claves del fenómeno de disruptividad tecnológica, analizando su impacto en el sector de la Defensa y haciendo un recorrido por las actividades desarrolladas en el ámbito internacional y nacional. Para finalizar, y como ejercicio de vigilancia, valoración y predicción tecnológica, una última sección revisa brevemente algunas de las áreas tecnológicas con mayor potencial de disruptividad.

Palabras clave

Tecnología disruptiva, Defensa, nivel de madurez tecnológica, vigilancia tecnológica, valoración tecnológica, predicción tecnológica, prospectiva, I+D, nanotecnología, robótica, bioingeniería, energía.

Abstract

Technology is an undeniable factor of transformational power on society as it has been showed up early in history. Nevertheless, the disruptive technology effect has even been able to fall over economic, social, political and ethics models. Defence is a clear example. This sector has historically been the cutting edge on technology development. High disruptive technology discoveries had made a sharp turn on power structures and world order.

Most nations, aware of distinguishing effect of technology, invest to a greater or lesser degree in the exercise of technology changes prediction coming in, the impact, benefits and cost. The goal is to exploit opportunities and mitigate risks attached to whether or not adopt a technology discovery.

In this chapter, the intention is to offer the keys on disruptiveness technology phenomenon, analysing its impact on defines and going across national and international activities around it. Finally, a short review of most potential disruptive technologies is shown in the last section as an exercise of technology watch, assessment and foresight.

Keywords

Disruptive technology, Defence, technology readiness level, technology watch, technology assessment, technology prediction, prospective, R&D, nanotechnology, robotics, bioengineering, energy.

¿POR QUÉ IMPORTAN LAS TECNOLOGÍAS DISRUPTIVAS EN DEFENSA?

Dado su ADN basado en la tradición, los ejércitos suelen prestar una gran atención a la innovación sostenida que privilegia las mejoras en las plataformas, sistemas de armas y modos de operar que consideran bien establecidos. Pero es obvio que nunca deberán descuidar nuevos modos de combatir alternativos, ya que correrían el riesgo de verse superados por sus rivales que sean capaces de sacar adelante amenazas basadas en procesos tecnológicos disruptivos.

Figura 1. La guerra no cambia, sí la tecnología. Fuente: http://foxtrotalpha.jalopnik.com

La verdad es que como cualquier otra organización ante entornos cambiantes, y cada vez más cambiantes, las tecnologías de las armas nunca evolucionan de un modo lineal sino que experimentan cambios tecnológicos que repercuten en toda su estructura y operaciones.

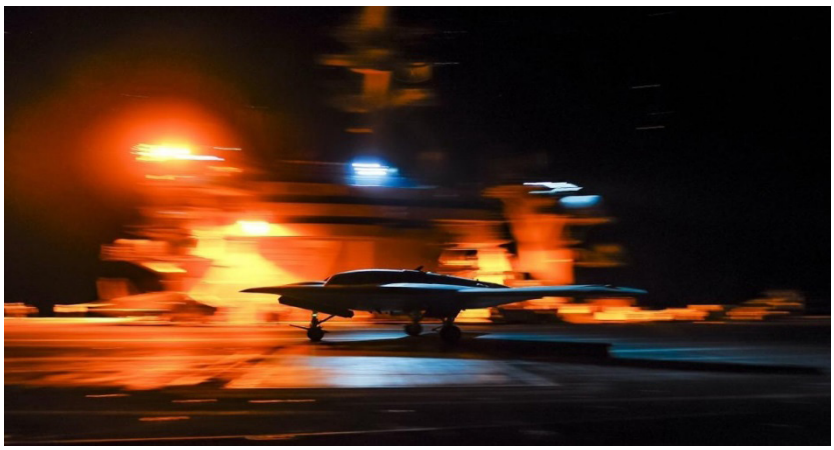


Figura 2. El futuro combate aéreo naval está marcado por la robótica. Fuente: http://foxtrotalpha.jalopnik.com

Debemos reconocer la valentía de haber apostado hace unas décadas por los teléfonos móviles frente a la telefonía fija o por el inmediato correo electrónico frente a los tradicionales envíos postales. Existen múltiples ejemplos de lo contrario en nuestro mundo de Defensa, de hecho no es difícil imaginarse la cara de horror de Napoleón cuando le dijeron que debía cambiar la propulsión de las velas de sus buques por un incendio controlado debajo de la cubierta. Y en nuestro caso, nos gusta imaginar que hubiera ocurrido si se hubiese apostado con firmeza por la tecnología expuesta por Blasco de Garay o por Isaac Peral.

La década de los sesenta nos aportó, además de a los Beatles, el interés de algunos de los países más desarrollados en evaluar tecnologías emergentes con el fin de identificar de forma temprana el impacto, los beneficios y costes de los cambios tecnológicos, ya que en ese momento se generalizó la conciencia de que cualquier cambio tecnológico llevaba inherente un riesgo, sirva como ejemplo de referencia la importancia de la fisión nuclear en la Segunda Guerra Mundial. Ya en los 70, los EEUU utilizaron la evaluación tecnológica como herramienta para la definición de políticas de desarrollo tecnológico y una década más tarde se instauró como herramienta de apoyo a la toma de decisiones a nivel gubernamental e industrial y se consolidó como un componente del proceso de definición de las estrategias y políticas de innovación (12) (2) (3).

En la actualidad se ha entendido y consolidado la actividad de vigilancia, evaluación, prospectiva y predicción tecnológica en la mayoría de los ejércitos, de modo que la tecnología forma parte de los procesos de planeamiento de Defensa desde sus etapas más prematuras consiguiendo con ello mayor eficacia en la toma de decisiones o lo que se resume como "cliente inteligente". Es evidente que la complejidad de este proceso reside en el componente de predicción requerido, ahí la prospectiva proporciona herramientas metodológicas que facilitan y sistematizan la reflexión colectiva y la construcción de imágenes o escenarios de futuro.

Aunque el concepto de "tecnología disruptiva" viene del ámbito empresarial, esencialmente del de la economía en su búsqueda de la predicción de cambios radicales, la aplicación al mundo de la Defensa es clara; no detectar a tiempo una tecnología disruptiva supone ignorar un factor de superioridad e incrementar el "gap" tecnológico respecto a los que sí la han asumido. Aunque el impacto de las tecnologías sobre un escenario futuro es difícil predecir, sin duda determinadas tecnologías marcan un antes y un después en la concepción de los diversos sistemas. En todos los sectores, incluido el de Defensa, la diferencia entre identificar y desarrollar una tecnología disruptiva y no hacerlo, supone un factor de superioridad que puede ser decisorio tanto en una situación de conflicto y constantemente como impacto disuasorio.

Dadas las muchas posibles fuentes de información, la tecnología es cada día más accesible y permite que surjan nuevas amenazas procedentes de regímenes ilegítimos, grupos terroristas y delincuencia organizada que acceden a ciberdelincuencia, armas de destrucción masiva, mercado negro armamentístico, etc. Esto implica un cambio en la idea de la amenaza tradicional procedente de enemigos identificados. La innovación

tecnológica está cada día más fuera del control de los estados debido a su progresiva democratización (1), más actores y mucha rapidez de acceso a la información.

Desde el cambio de paradigma de los años 70, cada vez más las tecnologías que se aplican en el ámbito de Defensa provienen del entorno comercial, habiéndose invertido la tendencia en la que los avances tecnológicos provenían principalmente de I+D efectuada en programas militares (9), (10), (11).

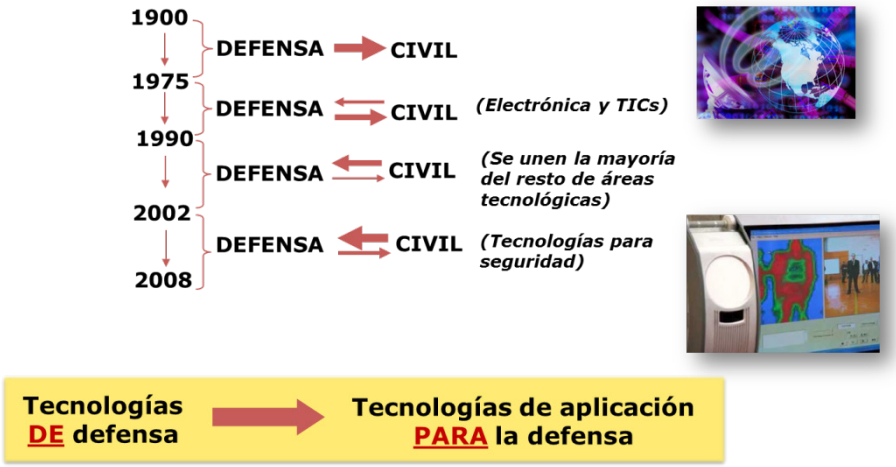


Figura 3 Evolución del liderazgo y trasferencias tecnológicas. Fuente: SOPT.

En la actualidad (6) es necesario afrontar una gran diversidad de amenazas potenciales de actores convencionales y entidades asimétricas, todos ellos presentan un grado creciente de incertidumbre, dispersión y complejidad y con una extensión paulatina del ámbito exclusivo de la Defensa a la seguridad de la sociedad civil y los sistemas económicos. Estas tres cualidades, incertidumbre, dispersión y complejidad, son un buen caldo de cultivo de disrupciones que obligan a adquirir capacidades de adaptación y reacción muy exigentes. Así que no sólo hay que mantener la capacidad de vigilancia, prospectiva, evaluación y gestión tecnológica sino que además hay que adaptar las estructuras organizativas y los procesos para atender las necesidades de obtención de los distintos sistemas que evolucionan con la demanda dinámica que exigen por la existencia de estos escenarios asimétricos.

En este contexto de Defensa y Seguridad, donde surgen continuamente nuevos desarrollos tecnológicos disruptivos (6), es cada vez más necesario el pensamiento innovador, nuevos conceptos operacionales, nuevos modelos organizativos y el establecimiento de estrategias a largo plazo, donde la tecnología se contempla como catalizadora de capacidades militares, con impacto tanto en la Fuerza como los propios conceptos de los sistemas. Ante estos desafíos, juega un papel fundamental la competitividad tecnológica industrial. El favorecer la competitividad de ideas, el fomento de la innovación y el alineamiento de las estrategias industriales y tecnológicas en Defensa con los objetivos definidos a medio y largo plazo.

Con este objetivo, el gobierno de los EEUU mantiene una apuesta firme por la tecnología como agente diferenciador de las capacidades militares y en noviembre de 2014 lanzó la nueva "Third Offset Strategy" (5), en la que se identifican las tecnologías clave que podrán mantener la supremacía disuasoria y en mantenimiento de paz en este nuevo ciclo de 20 años. Entre estas tecnologías identifican[22] la robótica y sistemas autónomos, la miniaturización, el big data y el empleo de técnicas de fabricación avanzada, donde juega un papel importante la impresión 3D.

Las organizaciones y alianzas internacionales en materia de Defensa, conscientes de la relevancia de la tecnología como factor clave del planeamiento de Defensa (19), (20), han puesto en marcha iniciativas dirigidas a un mismo objetivo, la vigilancia, valoración y predicción de tecnologías disruptivas que puedan tener impacto en materia de Defensa. La OTAN, por ejemplo, estableció actividades y grupos de trabajo (7), (8), y la EDA, puso en marcha en 2008 la iniciativa JIP-ICET (Joint Investment Programme on Innovative Concepts and Emerging Technologies).[23] (21)

A nivel nacional, el proceso de identificación de tecnologías, tanto emergentes como disruptivas, en el ámbito de Defensa se lleva a cabo en el Sistema de Observación y Prospectiva Tecnológica (SOPT), de la Subdirección General de Planificación, Tecnología e Innovación (SDGPLATIN) de la DGAM, con el apoyo de su red de colaboradores.[24]

SOPT

SISTEMA DE OBSERVACIÓN Y PROSPECTIVA TECNOLÓGICA

Figura 4. Logo del SOPT. Fuente. SOPT

22 http://breakingdefense.com/2014/11/hagel-launches-offset-strategy-lists-key-technologies/

23 http://www.eda.europa.eu/docs/default-source/eda-factsheets/jip-icet-factsheet_300113

24 http://www.tecnologiaeinnovacion.defensa.gob.es/

¿QUÉ ES UNA TECNOLOGÍA CON POTENCIAL DISRUPTIVO?

El origen anglosajón del concepto de "disrupción" puede identificarse de manera global con un cambio brusco con lo prestablecido, de forma que con algo nuevo se obtiene una enorme ventaja respecto a algo. Podemos considerar que una tecnología tiene un potencial disruptivo si tiene la capacidad de dejar a otra parcialmente obsoleta o inútil que obliga a cambiar la forma de operar de los usuarios y la industria. Así, se consideran como disruptivas las tecnologías que una vez disponibles cambian de manera relevante la forma de actuar. Algunos ejemplos recientes de tecnologías disruptivas son los teléfonos móviles o nuestros inseparables "WhatsApp", así como las descargas de vídeos, películas o música vía Internet. Otros casos como el IPad, las "tablets" o los drones, revolucionan el mercado y son disruptivos, convirtiéndose en sistemas de uso habitual y ahora se renuevan de manera evolutiva.

Figura 5. El comercio electrónico y la comunicación vía Internet han sido innovaciones disruptivas relevantes de nuestro siglo. Fuente: http://wikipedia.org

El término tecnología disruptiva fue empleado por primera vez por Clayton M. Christensen y su colega Joseph Bower, ambos profesores de Harvard Business School en el año 1995 en su publicación "Disruptive Technologies: Catching the Wave" (4). Posteriormente, en su obra "The Innovator's Dilemma" (5), Christensen definió la innovación disruptiva como el proceso por el cual un producto o servicio es adoptado en un principio tímidamente por el mercado para aplicaciones sencillas y repentinamente genera un vuelco y un cambio de tendencia en el propio mercado, llegando a desplazar a sus competidores iniciales, como lo ocurrido recientemente con la telefonía móvil que ha desplazado a la telefonía fija que teníamos.

Las innovaciones tecnológicas disruptivas no son evolutivas, ni lineales, e implican cambios revolucionarios, no son pequeñas mejoras sobre algo existente sino algo nuevo que deja como ineficiente o en desuso a lo anterior. Su diferencia con los cambios o innovaciones tradicionales es que estos suelen implicar pequeños cambios sobre un mismo sistema, nuevas versiones o integraciones tecnológicas en sistemas que mejoran la forma de trabajar. En nuestro ámbito, se define una tecnología disruptiva como el desarrollo tecnológico que en un corto periodo de tiempo es susceptible de provocar cambios sustanciales en la doctrina operativa de la Fuerza, especialmente en lo que

se refiere a las reglas de enfrentamiento, generando con ello un nuevo paradigma en los objetivos a largo plazo a nivel conceptual y estratégico, con un serio impacto en el planeamiento militar.

En la literatura encontramos diferentes términos en torno al poder transformacional de las tecnologías. Adicionalmente al ya definido "tecnología disruptiva", los más habituales son tecnologías emergentes, tecnologías convergentes o tecnologías habilitadoras. Todos estos términos refieren a conceptos ligeramente diferentes pero no excluyentes, de modo que una tecnología emergente pude ser disruptiva, convergente y habilitadora. Así, las tecnologías emergentes se refieren al efecto de emerger, son tecnologías con un escaso nivel de madurez que ofrecen expectativas de futuro, tienen potencial disruptivo si tienen la capacidad de promover cambios revolucionarios y desplazar tecnologías existentes.

Figura 6. Identificación y análisis de tecnologías. Fuente: JISC Observatory.

Tecnologías convergentes denotan la posibilidad de establecer sinergias entre dos o más tecnologías de forma que adquieran la capacidad de generar nuevas tecnologías y transformar los modelos de producción. Sin duda alguna, las tecnologías convergentes tienen también potencial disruptivo.

Por último, el término de tecnología habilitadora se asimila con el término capacitación, centrándose en la capacidad de una tecnología de habilitar, propiciar o catalizar el desarrollo, evolución, transformación o generación de bienes, servicios, tecnologías, etc. Por supuesto una tecnología habilitadora puede ser disruptiva, pero en este caso el foco es la capacidad de habilitar y no su carácter disruptivo.

IDENTIFICACIÓN Y ANÁLISIS DE LAS TECNOLOGÍAS CON POTENCIAL DISRUPTIVO

En el proceso de identificación y análisis tecnológico, a lo largo de las últimas décadas se han contrastado diversas implementaciones. Las técnicas genéricas de identificación de tecnologías más extendidas son la exploración del horizonte tecnológico, metodología de metascanning (15), muy empleada en gestión dinámica

de riesgos, el análisis de frecuencia de ocurrencias de conceptos clave, el juicio experto y la priorización.

En cuanto al análisis de las tecnologías, algunas prácticas reconocidas son la visión de expertos en el ámbito tecnológico y operativo, los estudios paramétricos -método Taguchi (16)-, que buscan las diferencias que marcan la diferencia basándose en funciones de pérdida asociada, la filosofía de control de calidad off-line y la innovación en el diseño de experimentos, los juegos de guerra, donde se exploran conceptos, tecnologías y escenarios sin limitaciones, los foros de discusión, incluyendo el método Delphi, los procesos analíticos jerárquicos para tratar de forma estructura decisiones complejas -Análisis Saatay (17)- o la aplicación de tecnologías a modelos existentes.

Pero la identificación y análisis tecnológico es insuficiente y debe ponerse el foco en el carácter disruptivo que marca la diferencia, por lo que es necesario analizar el contexto, las causas y efectos que promueven a una tecnología a ser disruptiva, y estas causas y efectos pueden no ser tecnológicos, por ello es necesario afrontarlo bajo un enfoque integral. Necesitamos considerar dos aspectos clave, que la disrupción es un proceso, no es un evento, aunque las disrupciones pueden ser lanzadas por eventos y que la disrupción es un fenómeno relativo, de modo que aquello disruptivo en un contexto puede no serlo en otro.

En Defensa, el carácter disruptivo de la tecnología tiene ciertas particularidades como que no es necesario que la tecnología sea nueva o emergente, ya que nuevos usos de tecnologías obsoletas o la combinación de tecnologías existentes (tecnologías convergentes) pueden tener impacto disruptivo o que tampoco es necesario superar en prestaciones a los sistemas existentes, tecnologías de prestaciones menores pueden ser decisivas si generan mejor rendimiento a los sistemas en uso por diversos motivos como la aceptación social, la adaptabilidad a las amenazas, a los puntos débiles de los adversarios, etc.

Respecto al potencial disruptivo, en la identificación de una tecnología, en su valoración pueden tenerse en cuenta (18) (14) como que la tecnología puede existir o ser nueva, de hecho, nuevos usos de tecnologías maduras y/u obsoletas pueden causar disrupción, que puede tener características similares (en prestaciones, en calidad, etc.) a las soluciones tecnológicas existentes, pero proporciona unas funcionalidades adicionales o que no tiene que necesariamente desplazar significativamente a las soluciones tecnológicas existentes para causar disrupción. Y hay otros factores adicionales al tecnológico, como son el momento cronológico, las circunstancias sociales, de comportamiento, etc. Además en Defensa, hay que añadir otros factores influyentes como que la efectividad militar se valora y se evalúa de modo diferente a la rentabilidad comercial y los aspectos éticos y legales toman dimensiones diferentes.

A nivel nacional, la realización de actividades de vigilancia tecnológica que permiten conocer el estado del arte de las soluciones tecnológicas, la identificación de tecnologías emergentes, el conocimientos de los actores y sus capacidades y el apoyo en una red

muy cercana de colaboradores y expertos, ayudan a una identificación temprana de posibles tecnologías con alto potencial disruptivo.

La importancia de identificación y análisis de las tecnologías con potencial disruptivo se pone de manifiesto en la creación de diferentes grupos de trabajo en las organizaciones internacionales en las que formamos parte (LoI, EDA y STO) que pretenden poner en común los enfoques de los distintos países a la hora de detectar tecnología disruptivas, y facilitar el intercambio de información entre los expertos sobre cuáles son las tecnologías que se prevén como disruptivas en los próximos años.

Existen diferentes aproximaciones metodológicas a la hora de abordar la identificación y análisis del potencial carácter disruptivo de las tecnologías (xx), consideramos aproximación "bottom-up" (de abajo a arriba) que partiendo de tecnologías y su potencial carácter disruptivo prevé su impacto en los futuros sistemas y capacidades y aproximación "top-down" (de arriba a abajo) que parte de la identificación de capacidades y efectos disruptivos deseables así como de las tecnologías y sistemas que ofrecerían dichas capacidades y producirían tales efectos.

LA PROSPECTIVA COMO HERRAMIENTA DE BASE

Para profundizar en un análisis de qué son y para qué sirven las tecnologías disruptivas es necesario exponer una de las herramientas que mayor desarrollo ha tenido en los últimos años, la prospectiva (13), la cual constituye un elemento de apoyo a la decisión en la planificación estratégica y tecnológica de valor incalculable. En referencia a su definición, la RAE define la prospectiva como el "Conjunto de análisis y estudios realizados con el fin de explorar o de predecir el futuro, en una determinada materia".

La prospectiva emplea herramientas que sistematizan la reflexión sobre el futuro. Estas herramientas tienen como principal función la de analizar cuál puede ser la evolución de las tecnologías clave y qué variables pueden incidir sobre la misma. El resultado de la aplicación de estas herramientas modificado por las variables de contorno que puedan afectar al resultado final. Pero como es lógico, es preferible tener una cierta previsión sobre cómo puede evolucionar el futuro que no hacer ningún tipo de previsión sobre él, y de aquí la función de la prospectiva. Los métodos generalmente más empleados a la hora de realizar "prospectiva tecnológica" son la extrapolación, entendida como el intento de extender al futuro pautas de comportamiento observadas hasta el momento, el empleo de variables correlacionadas, la aplicación de modelos causales, el uso de métodos probabilísticos, que implica la asignación de determinadas probabilidades para las diferentes alternativas y los métodos interactivos, que infieren los resultados del análisis de la información que realizan expertos en la materia.

El empleo de todos ellos supone la base de un estudio adecuado, ya que todos los métodos expuestos cuentan con sus ventajas e inconvenientes, y sobre todo que

la prospectiva no es una ciencia, no hace milagros, ni adivina el futuro, sólo es una herramienta que nos ayuda en la toma de decisiones reduciendo la incertidumbre existente.

Figura 7. La prospectiva evalúa alternativas futuras. Fuente: "Minority report""

Es posible citar algunas técnicas para realizar prospectiva como el análisis de patentes, vigilancia de tecnologías disruptivas, cienciometría, scoutismo tecnológico, etc. A modo de ejemplo es posible señalar el empleo de indicadores bibliométricos o cienciometría como parte de la explotación estadística de datos científicos y tecnológicos, que permite estudiar la incidencia que determinada disciplina tecnológica tiene entre los trabajos de la comunidad investigadora, y por tanto los recursos que a priori se están destinando, el número de patentes que se publican sobre una determinada línea o qué empresas están detrás de tales trabajos.

Así, el empleo de la prospectiva permite reducir el riesgo en la puesta en marcha de una iniciativa, proyecto, etc. y permite identificar los factores clave para que se implemente la estrategia que articule las acciones que nos permitirán interpretar el entorno, visualizar los escenarios previsibles, y reconocer las tendencias, potencialidades y elementos disruptivos que afectan al desarrollo tecnológico.

EXPERIENCIAS PREVIAS DEL MDEF EN ORGANISMOS INTERNACIONALES: LoI, NATO Y EDA

LoI/FA EDIR (Letter of Intent-Intentions / Framework Agreement for European Defence Industrial Restructuration) conocida para su simplificación como LoI (20) hace referencia a un tratado que se firmó el 27 de julio del 2000 en Farnborough entre Francia, Alemania, Italia, España, Suecia y Reino Unido. Su misión es facilitar la restructuración de la industria europea de Defensa, con el fin de promover una base tecnológica e industrial más potente y competitiva.

El Ministerio de Defensa participa en los asuntos de I+T en el marco de la LoI por medio del grupo GRD (Group of Research Directors), que tiene el objetivo de fomentar la coordinación de actividades de investigación en cooperación con el fin de incrementar la base de conocimiento y de estimular el desarrollo e innovación tecnológica. El GRD crea grupos de trabajo específicos para profundizar en iniciativas de ámbitos tecnológicos concretos. Actualmente hay dos grupos en activo, entre los que se encuentra el Grupo de Tecnologías Disruptivas (DTG: Disruptive Technologies Group). Cabe destacar la participación de Holanda en el DTG aun no siendo miembro de la GRD.

El principal objetivo del DTG es proporcionar asesoramiento tecnológico al Grupo de Directores de I+T de la LoI, poniendo en común los enfoques de los distintos países y facilitando el intercambio de información sobre este tipo de tecnologías. Desde 2009, y bajo el liderazgo de la Subdirección General de Planificación, Tecnología e Innovación (SDGPLATIN) de la DGAM, el grupo ha definido e implantado un proceso propio para la identificación de tecnologías con potencial de disrupción. Este proceso parte de todo el espectro tecnológico para, después de aplicar varios filtros, poder llegar a la identificación de tecnologías disruptivas como muestra la Figura 8.

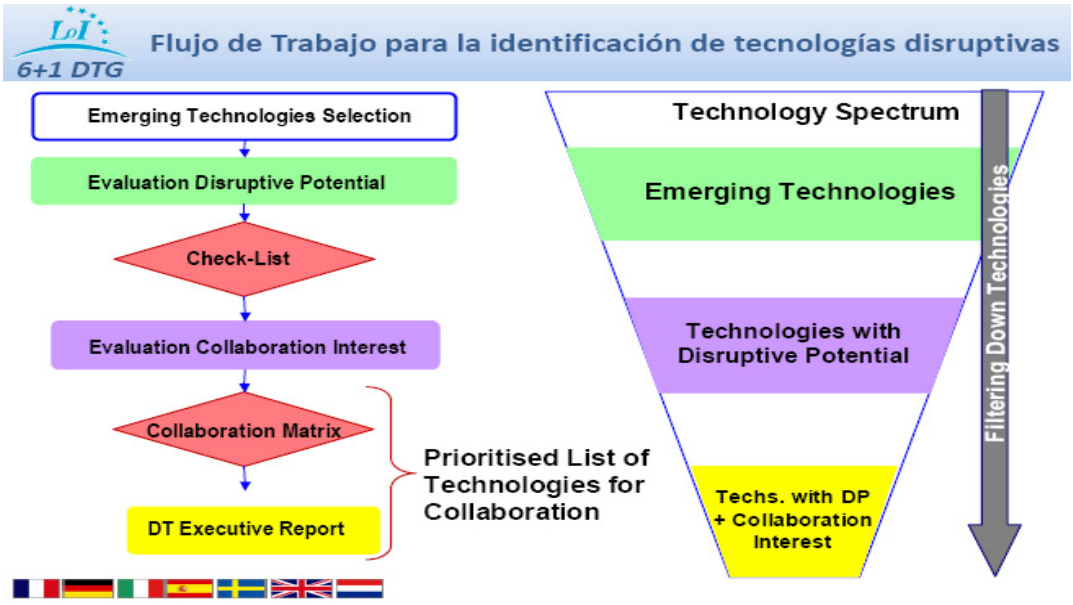


Figura 8. Flujo de trabajo de la LoI. Fuente: (20).

El procedimiento comienza tomando de partida un conjunto de tecnologías emergentes identificadas por el grupo, tecnologías con bajos niveles de madurez tecnológica, lo que supone el primer filtro y se analizan para identificar aquellas que tengan mayor potencial de disrupción en un segundo filtro. Por último, en la fase final, se identifican las áreas tecnológicas de interés donde lanzar actividades de cooperación a nivel europeo. Estas áreas se seleccionan a partir de la lista completa de tecnologías disruptivas, seleccionando las que tienen mayor interés al estar alineadas con el Plan a Largo Plazo de Armamento y Material (PLP-AM) y la Estrategia de Tecnología e Innovación para la Defensa (ETID) y en las que existe cierta capacidad tecnológica nacional.

La Organización de Ciencia y Tecnología de la OTAN (STO – Science and Technology Organization) (19) reconoció hace varias décadas la importancia de identificar aquellas tecnologías que poseían un elevado potencial de disrupción, tanto si suponen una oportunidad para las Fuerzas de la Alianza como si implican una amenaza para dichas Fuerzas. Como prueba de este interés destacar tres hechos de especial relevancia:

- Los 7 Paneles Técnicos en los que la STO organiza sus actividades (AVT, HFM, IST, SAS, SCI, SET y MSG)[25] tienen como una de sus funciones habituales la realización de Vigilancia Tecnológica ("Technology Watch") para la identificación de innovaciones científicas o técnicas que puedan tener un efecto disruptivo en el ámbito militar.[26]

- Desde hace años, las prioridades de ciencia y tecnología de la Organización recogen de manera específica las denominadas E2DT ("Emerged/Emerging Disruptive Technologies").[27] Esta lista de tecnologías emergentes con alto potencial disruptivo pretende estimular la exploración e identificación de aplicaciones innovadoras que, utilizando dichas tecnologías y en conjunción con los cambios adecuados en las tácticas y lo procedimientos, puedan proporcionar una ventaja operativa significativa al ejército que las utilice. Asimismo, es interesante señalar que uno de los dos requisitos en los que se ha basado la identificación de las nuevas prioridades de Ciencia y Tecnología de la OTAN[28] ha sido el potencial de disrupción tecnológica asociado a dichas prioridades.

- En el marco de la STO, se han lanzado diversos grupos de trabajo "technical teams" sobre tecnologías disruptivas. De estos grupos, podemos destacar el SAS-062 "The Impact of Potentially Disruptive Technologies" (7) y el SAS-082 "Disruptive Technology Assessment Game: Extension and Applications" (8), los cuales contaron con la participación del Ministerio de Defensa a través de la SDGPLATIN de la DGAM. Estos grupos se centraron en la identificación de posibles tecnologías disruptivas aplicables a Defensa y Seguridad, para lo cual pusieron en práctica una metodología basada en modelos de juegos estilo "wargame" para la evaluación de las tecnologías identificadas. En estos juegos participaron tanto operativos, como tecnólogos y analistas.

25 AVT - Applied Vehicle Technology; HFM - Human Factors and Medicine; IST - Information Systems Technology; SAS - System Analysis and Studies; SCI - Systems Concepts and Integration; SET – Sensors and Electronics Technology; MSG – Modelling and Simulation Group.

26 STO Collaborative Network Operating Procedures. 1st Issue, June 201CSO/DIR(2013)0020.

27 2014 STB Science & Technology Priorities. AC/323-D(2014)0003.

28 Aprobadas en enero de 2015 NATO Science & Technology Priorities. AC/323-D(2015)0001

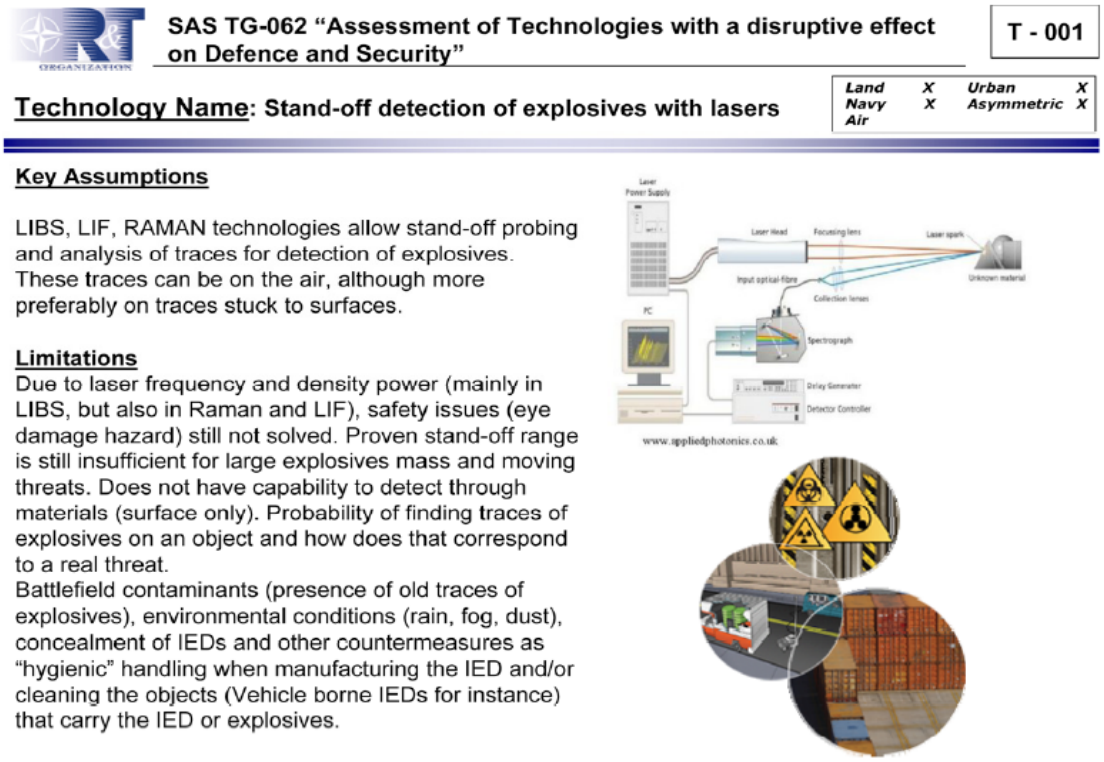


Figura 9. Modelo de tarjeta sobre tecnología. Fuente: GT SAS-062.

A finales del año 2008 la Agencia Europea de Defensa (EDA) puso en marcha el programa de inversión conjunta JIP-ICET (Joint Investment Programme on Innovative Concepts and Emerging Technologies)[29] (20) (21). Esta iniciativa tenía como objetivo aumentar el esfuerzo en investigación básica en Defensa que se realiza en Europa, promoviendo la investigación en tecnologías emergentes que pudieran tener un efecto disruptivo en las futuras operaciones europeas. Los proyectos que se lanzaran bajo el paraguas de JIP-ICET serían iniciativas de I+D de alto riesgo y bajo nivel de madurez tecnológica (TRL), que difícilmente un solo país podría financiar.

Se establecieron tres áreas principales ("technological clusters") hacia las que dirigir los esfuerzos, cada una con una serie de objetivos de I+T o "R&T goals":

29 https://www.eda.europa.eu/docs/default-source/eda-factsheets/jip-icet-factsheet_300113.

Technological Cluster	R&T Goal
ICET-A: Improved Autonomy	ICET – A1 : Non Linear Control Design
	ICET – A2 : Integrated Navigation Architecture
ICET-B : New Solutions for Materials and Structures	ICET – B1 : Nanotechnologies
	ICET – B2 : Structural Health Monitoring
ICET-C : Data Capture and Exploitation	ICET – C1 : Remote Detection of Hidden Items
	ICET – C2 : Nanostructures Electro-Optical and other
	ICET – C3/1 : Radar Technologies / Processing
	ICET – C3/2 : Radar Technologies / Components

Tabla 1 Áreas objetivo de esfuerzo I+T. Fuente JIP-ICET.

En el programa JIP-ICET participaron 11 países europeos: Alemania, Chipre, Eslovaquia, Eslovenia, Polonia, Francia, Grecia, Hungría, Italia, Noruega y España, contribuyendo con un presupuesto total de 15,5M€, de los cuales España aportó 2M€. Como resultado de las tres convocatorias de proyectos que se lanzaron entre 2008 y 2010, se contrataron 12 enfocados a temas como la monitorización de la salud estructural del fuselaje de helicópteros, la utilización de radares SAR para ayuda a la navegación de aeronaves, sistemas de radares pasivos, componentes ópticos nanoestructurados para detección CBRN y enlaces ópticos, detección a distancia de explosivos por medio de ondas de Terahercios, la aplicación de los metamateriales o el estudio prospectivo sobre la integración de los nanomateriales en los textiles.

La participación en el JIP-ICET fue muy provechosa para España, ya que las entidades nacionales participantes: industria, universidades y centros de investigación consiguieron un retorno del 112% respecto a la inversión realizada por el Ministerio de Defensa. Un total de 10 entidades españolas participaron en 7 de los 12 proyectos contratados, liderando 5 de ellos. El éxito del programa motivó el lanzamiento, en enero de 2013, de su continuación bajo el acrónimo JIP-ICET 2 con los siguientes objetivos de I+D: inteligencia artificial, nuevos conceptos de cooperación hombre-máquina, tecnologías de almacenamiento energético, criminología (bioterrorismo y microbiología forense), redes de sensores y sistemas de captación de energía para el combatiente, controles activos para flujos y mezclas de gases, entorno espacial, verificación y validación de sistemas analógicos y digitales distribuidos.

El JIP-ICET 2 constituyó un excelente ejemplo de las sinergias y el nivel de colaboración existente entre el GRD de la LoI y la EDA. De hecho, el GRD tras obtener los resultados del Grupo de Tecnologías Disruptivas, propuso a la EDA continuar con el programa.

La EDA está orientando sus trabajos de manera preferente a las denominadas "Tecnologías Críticas de Defensa" (CDT- Critical Defence Technologies). Una CDT se puede definir como una tecnología que sustenta una capacidad de Defensa europea que es estratégica hoy o lo puede ser en el futuro, y en la que la falta de inversión puede poner en riesgo la capacidad europea para la fabricación de sistemas basados en dicha tecnología. El concepto de CDT tiene un alcance más amplio que el de las tecnologías disruptivas, y comprende varios aspectos que están interrelacionados: dependencias tecnológicas, tecnologías emergentes y potencial de disrupción, entre otros.

Los trabajos en las CDT se fundamentan en las iniciativas desarrolladas previamente por la Agencia sobre Independencia Tecnológica Europea (ETnD – European Technology Non-Dependence), tomando también como referencia los trabajos de la Comisión Europea en las Tecnologías Facilitadoras Clave (KET - Key Enabling Technologies) y los avances de la Agencia Espacial Europea (ESA) en la definición de las Tecnologías Espaciales Críticas. A nivel de la propia EDA, también se han tenido en cuenta las Agendas Estratégicas de Investigación (SRA – Strategic Research Agenda) de cada uno de sus 12 Capabilty Technology groups "CapTechs".[30] (22)

En junio de 2014, la Junta Directiva de la EDA refrendó la primera lista de CDT y encomendó a la Agencia la actualización de dicha lista con una periodicidad anual, a través del establecimiento de un proceso que permita determinar dichas CDT de manera sistemática. Para poder cumplir este cometido, la EDA ha puesto recientemente en marcha un Grupo de Trabajo sobre CDT, en el que participan expertos de las naciones de la EDA y que involucra también al personal de la Agencia encargado de apoyar y coordinar internamente el trabajo de los CapTechs. Este grupo de trabajo es el encargado de validar el proceso para la identificación de las CDT que define la Agencia.

En la cooperación entre la LoI y la EDA, el DTG de la LoI trata de adaptar el proceso que han desarrollado para la identificación de las tecnologías disruptivas a las necesidades del grupo de trabajo sobre CDT. Asimismo, se mantiene una cooperación continua con la ESA en las Tecnologías Críticas Espaciales y con la Comisión Europea en lo que se refiere a las KET, sin dejar de promover los temas relacionados con ETnD. Para evitar duplicidades, también se tendrá en cuenta las actividades de la OTAN en esta área, como por ejemplo las relacionadas con "Horizon Scanning" (15).

30 http://www.eda.europa.eu/randtuserguide/home/captechs.

ALGUNAS ÁREAS CON POTENCIAL DE DISRUPCIÓN

Armas de energía dirigida mediante láser de alta potencia

Las armas de energía dirigida mediante láser emiten energía electromagnética en diferentes rangos espectrales (principalmente visible e infrarrojo) a un objetivo preciso, y no lanzan ningún tipo de proyectil.

Una vez creadas, instaladas y totalmente operativas, este tipo de armas simplemente consumen energía eléctrica (transforman la energía eléctrica en radiación electromagnética), por lo que no necesitan munición convencional. Su uso generalizado y adaptado a las aplicaciones de defensa implicaría un cambio logístico disruptivo, ya que se puede considerar que tienen munición "infinita", sin necesidad de recargas continuas ni proyectiles, y al necesitar simplemente una fuente de energía eléctrica podrían funcionar mediante energía solar fotovoltaica (u otro tipo de fuente). Una vez instaladas, sin tener en cuenta los costes de fabricación y desarrollo su uso es mucho más económico que las convencionales. Las armas convencionales gastan proyectiles de un coste diverso en cada disparo, mientras que un "disparo" de un arma láser tiene un coste muy inferior a un euro.

Además, al viajar los pulsos emitidos a la velocidad de la luz, a la hora de apuntar a los objetivos, no es necesaria ninguna corrección en las trayectorias de disparo, incluso aunque los objetivos sean RPAs o misiles. Tampoco requieren correcciones debidas al viento o a la gravedad, lo que hace que la trayectoria de los "disparos" sea lineal y por tanto el apuntamiento sea sencillo. En cuanto a la versatilidad de sus aplicaciones, los láseres de última generación tienen la capacidad de modificar la longitud de onda y la potencia en la emisión de sus pulsos. Esto hace que un mismo sistema se adapte para diferentes tipos de objetivos, incluso se puede llegar a adaptar al nivel de daño que se le quiera causar al objetivo. Respecto de su precisión, es muy alta, y salvo error en la discriminación de los objetivos, es muy difícil crear daños colaterales. Evidentemente, las armas láser no están clasificadas como armas de destrucción de áreas de manera indiscriminada.

Sus potenciales aplicaciones militares son múltiples, las más relevantes son contramedidas de misiles o morteros; destrucción de plataformas aéreas, principalmente RPAs; Autoprotección de buques, por ejemplo de ataques suicidas desde pequeñas embarcaciones; debido a su potencia y precisión, se podrían utilizar contra francotiradores y tropas de infantería, aunque habría que tener en cuenta los posibles problemas legales y éticos; y por último aplicaciones no letales, como inutilización de algunas plataformas terrestres.

Respecto del estado del arte, existen proyectos en curso en Estados Unidos y Europa, que cuentan con prototipos de armas láser en un estado de madurez muy avanzado. Algunos ejemplos son MBDA, en colaboración con BAE Systems, EADS y Finmeccanica, la US Navy o el U.S. Army Space and Missile Defense Command (SMDC) en colaboración con Boeing.

No obstante todavía quedan importantes retos que se deben resolver para obtener sistemas finales totalmente operativos, capaces de cubrir las necesidades de defensa, y convertirse en una nueva tecnología disruptiva que deje obsoletas a una parte relevante de las armas de munición convencional.

A día de hoy es difícil estimar el impacto final que tendrán las armas láser en los sistemas futuros, así como las aplicaciones en las que tendrán un éxito considerable y serán capaces de sustituir total o parcialmente, a las armas convencionales. Evidentemente, esto dependerá de hasta qué grado se consiguen resolver los siguientes retos tecnológicos:

- La energía emitida por el láser es absorbida y dispersada por el aire, lo que desenfoca y debilita el haz. Este efecto se multiplica cuando además hay partículas en el aire (niebla, humo, humedad, lluvia, polvo etc…). Por tanto, la energía que llega al objetivo disminuye enormemente respecto de la emitida con la distancia, lo que hace que la energía inicial ha de ser enorme.
- Cuando el láser alcanza al blanco, éste no resulta destruido instantáneamente, sino que va calentándose con rapidez pero de manera progresiva y de fuera hacia adentro. En el momento en que empiezan a evaporarse las primeras capas de material exterior del objetivo, éstas producen una neblina de ablación, que viene a provocar un "segundo florecimiento" en los últimos milímetros del recorrido. Obviamente, esto desenfoca y debilita también el haz, impidiéndole que siga destruyendo el blanco y permitiéndole enfriarse de nuevo.
- La necesidad de alta potencia de los láseres hace que los equipos de alimentación y refrigeración tengan volúmenes y pesos muy grandes. Esto dificulta su instalación en múltiples plataformas, especialmente en las aéreas.
- Podría ser fácil diseñar y aplicar contramedidas eficaces, como la generación de humos entorno al blanco, así como la pintura reflectante o el diseño de formas que tiendan a la dispersión de la energía incidente.
- Una vez emitidos los pulsos, al llegar al objetivo u objetos sólidos, una parte de la energía que llega es reflejada, lo que puede ser un riesgo para los ojos de los operativos, que podrían quedar total o parcialmente cegados. Hay que tener en cuenta que en las longitudes de onda visible e infrarrojo cercano, en las que trabajan la mayoría de los láseres, los ojos humanos son muy vulnerables.

No obstante, las grandes naciones industrializadas consideran que los retos tecnológicos son asequibles, al menos hasta un cierto punto en el que las armas láser

resulten de utilidad y sean potencialmente disruptivas, lo que se comprueba con las grandes inversiones que están realizando.

Figura 9. Prototipo de arma láser de estado sólido en el USS Ponce. Fuente: http://www.huffingtonpost.com/2013/04/09/us-navy-laser-weapon-deployed-uss-ponce-2014_n_3043244.html.

Autonomía, robótica y bioingeniería

La Biomímesis (23) o tecnología inspirada en la naturaleza puede inspirar a la mejora de muchos de nuestros sistemas y a ayudar a la humanidad a reducir el impacto sobre el medioambiente y a mejorar nuestra calidad de vida. Es por ello que se ha convertido en una de las áreas tecnológicas con mayor potencial disruptivo en multitud de sectores como son la arquitectura, automoción, etc., y como no en Defensa. Muchos de los retos e inversiones actuales para combatir las amenazas globales cambiantes en el contexto de Defensa se centran en el empleo de materiales bio-inspirados, principalmente para protección del combatiente, monitorización de áreas contaminadas, vigilancia, reconocimiento y tareas de rescate en zonas de difícil acceso.

En biología, algunas áreas a partir de las cuales se pueden modelar soluciones tecnológicas son la replicación de métodos naturales de manufactura como en la producción de compuestos químicos por plantas y animales, la imitación de los mecanismos encontrados en la naturaleza como el velcro y la cinta gecko y de los principios de organización social de organismos como hormigas, termitas y abejas.

Las líneas de I+D en este ámbito se centran principalmente en el desarrollo de músculos artificiales (la Universidad de Illinois ya dispone de un prototipo que se mueve por impulsos eléctricos y que se inspira en el funcionamiento del conjunto tendón y hueso) que podrían ser implementados en la próxima generación de biorrobots para administración de medicinas, cirugía e implantes inteligentes. También se están

desarrollando brazos biónicos (la empresa DEKA[31] ya ha comercializado un brazo de estas característicos que se controla mediante electrodos). Otro avance tiene relación con la regeneración celular, llevado a cabo por investigadores del hospital Mount Sinai de Nueva York basado en la capacidad que tienen algunos animales, como la salamandra o el pez cebra, para regenerar músculo cardiaco dañado.

Otro ejemplo de producto comercializable son las superficies de recubrimientos de la empresa Sharklet Technologies, para inhibir la contaminación bacteriana, inspirándose en los mecanismos naturales de los tiburones (Figura 10). Estos productos permiten la reducción de costes hospitalarios de entre 8.000 y 15.000 dólares por paciente.

Figura 10. Superficies libres de microorganismos, inspirándose en los tiburones Fuente: http://safetouchsolutions.net/technology/.

Biosensores para mejorar el diagnóstico de determinadas enfermedades o nanofármacos más especializados son otras aplicaciones que podemos encontrar. Un ejemplo reseñable en el ámbito nacional es el desarrollo del Instituto de Bioingeniería de Cataluña, de implantes biodegradables que ayudan al cerebro a autoregenerarse. Su trabajo ha sido publicado en la revista Biomaterials.[32]

Los avances en tecnologías 3D, el empleo de dispositivos láser para medición de distancias, la utilización de pequeños radares de localización de objetos próximos y los sistemas GPS de posicionamiento global, contribuirán a que para el 2025 se disponga de vehículos autónomos en el mercado. Un ejemplo de como en este sector ha copiado a la naturaleza son los coches autónomos que tratan de observar su posición con ojos parecidos a los de las abejas, debido a que su campo de visión es muy amplio cercano a los 300 grados. Este es uno de los objetivos del proyecto EPORO (EPisodio o RObot) que ha lanzado la compañía NISSAN (Figura 11). Con este mismo objetivo, la compañía ha estudiado los patrones de comportamiento de los peces, para analizar la fórmula por la que los distintos coches pueden interactuar entre ellos sin llegar a chocar.

31 http://www.dekaresearch.com/deka_arm.shtml.

32 http://dx.doi.org/10.1016/j.biomaterials.2014.02.051 0142-9612/ 2014 Elsevier Ltd.

Figura 11. Prototipo vehículo autónomo desarrollado por Nissan (Fuente: http://www.autobild.de/bilder/nissanrobbyepor0992398.html).

Los avances en inteligencia artificial, procesamiento de imágenes, sensores, motores y sistemas hidráulicos incrementarán las capacidades y complejidad de los robots. Algunos de los prototipos que se han desarrollado mimetizan peces o crustáceos para la monitorización de contaminantes en ambientes acuáticos, detección de minas, etc. En el desarrollo de un robot, la ingeniería y la biología se han puesto de acuerdo para avanzar y promover una disciplina conocida como 'soft robotics'. Este campo tiene promueve que los robots del futuro sean máquinas seguras, y para ello, deban estar compuestos de materiales blandos y ligeros. El Instituto de Tecnología de Massachusetts, ha desarrollado un pez robótico de silicona llamado 'Bubbles',[33] imitación de una carpa real, se trata del primer robot autónomo que consta principalmente de partes blandas. Las principales aplicaciones de este tipo de robots en el futuro podrían ser en búsqueda y rescate en zonas de naufragios. Otro ejemplo del empleo de materiales blandos y ligeros en el desarrollo de robots es el prototipo de la Universidad de Harvard y la de Cornell con forma de "X" o de cromosoma, y se ha ideado para que pueda variar su forma y ser resiliente ante condiciones climatológicas muy adversas como una tormenta de nieve o un fuego, haciéndolo idóneo para su uso en zonas peligrosas lo que además es propiciado gracias a su autonomía.

Otra línea de investigación de interés se centra en el desarrollo de nanobots en aplicaciones desde un uso para combatir el cáncer (Instituto Tecnológico de California), atacando genes específicos en las células malignas, desactivando sus funciones y destruyéndolas, como para su empleo en rescate en zonas de desastre para acceder a zonas de difícil acceso o en el espacio. La Universidad de Harvard ha creado pequeños robots que se comportan siguiendo el principio básico de construcción de las termitas, que captan el entorno inmediato y señales limitadas de los otros ejemplares para crear estructuras mayores, y aunque alguno de estos robots sea destruido, el resto podría finalizar su misión.[34]

33 http://newsoffice.mit.edu/2014/soft-robotic-fish-moves-like-the-real-thing-031 y https://www.youtube.com/watch?v=BSA_zb1ajes..

34 http://www.eecs.harvard.edu/ssr/projects/cons/termes.html, y http://wyss.harvard.edu/viewpage/358/.

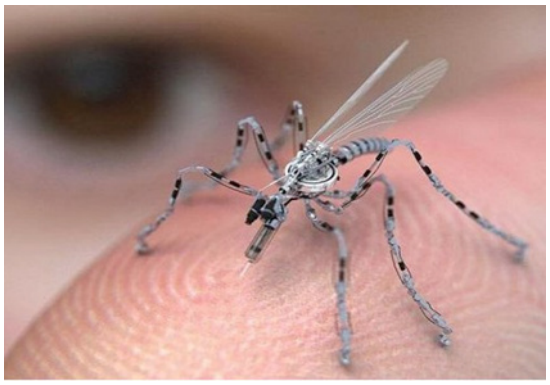


Figura 12. Drones espías que imitan mosquitos. (Fuente. http://esp.rt.com/actualidad/public_images/433/4330ed76903ee4e7b9a4c16139e89497_article.jpg.

Otro ejemplo de área con especial potencial disruptivo es el de los drones, cuyo origen exclusivamente militar ahora está extendido en el sector civil consecuencia de la reducción de precio de este tipo de dispositivos. Los hay de todo tipo, por citar algunos ejemplos están el *Bionic Bird,*[35] primer drone en forma de pájaro, que se controla desde un teléfono inteligente y es capaz de volar imitando el vuelo de un ave, lo que permite su camuflaje para operaciones de Defensa. Otro ejemplo son los microdrones y nanodrones que emulan tanto pájaros, como insectos (Figura 14) y otros animales pequeños, dirigidos a aplicaciones de vigilancia, siendo capaces de maniobrar a través de calles, pasillos y escondrijos. Estos sistemas podrían estar equipados con armas, sensores, cámaras de video, dispositivos de escucha, etc. Actualmente, se están empleando nanodrones en misiones militares de las fuerzas NATO en Afganistán que simulan ser insectos y cuya misión principal es el reconocimiento de escondites y calles que impliquen un riesgo para las tropas.

Figura 13. Robótica e inteligencia artificial tendrán un impacto disruptivo en la concepción del combate y reglas de enfrentamiento. Fuente: Call of Duty Wallpaper.

35 http://techcrunch.com/2014/11/05/bionic-bird/.

Nanotecnología

La nanotecnología presenta un amplio espectro de tecnologías prometedoras de gran potencial disruptivo (25). Hablar de nanotecnología es tratar el diseño, caracterización, producción y aplicación de estructuras, dispositivos y sistemas mediante el control del tamaño y la forma a una escala que va aproximadamente desde 1 a 100 nanómetros (nm). La nanotecnología permite la obtención de nuevos materiales con propiedades electrónicas, magnéticas, ópticas o mecánicas superiores a los materiales convencionales. Esto es debido a que a escala nano, la materia tiene una mayor área superficial por unidad de masa, lo que significa que tienen mayor superficie disponible para interaccionar con los materiales que les rodean. A escala nano se producen fenómenos físicos relacionados con efectos cuánticos que no ocurren a escala macro y que causan la variación de las propiedades de la materia anteriormente mencionadas.

Estas propiedades han despertado un gran interés en diferentes sectores como el de la salud, el transporte, la electrónica, el energético y por supuesto, el de la Defensa, con una gran versatilidad de aplicaciones. Particularmente son de especial interés aquellos nanomateriales en forma de partícula, fibra o lámina dirigidos a mejorar la protección y la seguridad del combatiente y a la reducción de peso y costes.

En el ámbito de la protección balística, se espera que nuevos materiales más ligeros y flexibles mejoren el nivel de protección del soldado frente a todo tipo de amenazas. También se espera un gran salto tecnológico en los blindajes dirigidos a integrar en plataformas terrestres, aéreas y navales, mejorando su resistencia estructural y reduciendo su peso. Esta es especialmente importante en el ámbito militar, ya que mejora la capacidad operativa del soldado (mejora del confort y movilidad, reduce la fatiga, etc.) y de las plataformas, sin pérdida de prestaciones y mejorando aspectos logísticos (consumos, transportabilidad, autonomía, etc.)

El desarrollo de la nanotecnología también permitirá la obtención de nuevos sensores más eficientes, con mayor capacidad de detección de agentes NBQ&E (Nucleares, Biológicos, Químicos y Explosivos), más selectivos y sensibles. Del mismo modo, con la miniaturización de los componentes electrónicos se conseguirá la obtención de sistemas que puedan ir integrados en el propio uniforme del soldado o en la estructura de una plataforma y que sean capaces de determinar si dicho soldado o dicha estructura se encuentra en condiciones de participar en una misión.

Además de las aplicaciones mencionadas anteriormente, la nanotecnología en Defensa puede tener un papel disruptivo en otros muchos campos como por ejemplo en la capacidad de disminuir la detectabilidad de los sistemas de Defensa mediante una reducción de la firma radar, infrarroja, acústica, etc. en la mejora de la eficiencia de los sistemas de generación y almacenamiento de energía, en el desarrollo de nuevos recubrimientos que mejoren la protección frente a la degradación de las plataformas, y

en general, en la generación de nuevos materiales con nuevas multifuncionalidades tan sorprendentes como la autorreparación, la capacidad de mantener el confort térmico en condiciones climáticas extremas, autolimpieza, etc.

Figura 14. La miniaturización de sistemas será posible gracias a nuevos métodos de fabricación a escala nano. Fuente: http://www.taringa.net/posts/ciencia-educacion/13793025/Nanotecnologia-mejorara-nuestra-calidad-de-vida.html.

Energía: generación y almacenamiento en campamentos y armas

El papel de la energía en Defensa puede analizarse desde varios ángulos. Comenzando en un plano general, la energía tiene un papel fundamental a nivel geoestratégico.[36] La consciencia de su importancia ha hecho que las estrategias de seguridad nacional de España y otros países de nuestro entorno incluyan la seguridad energética. Otro ámbito en el que la energía supone un factor clave es en la logística para el mantenimiento de operaciones. El crecimiento del número de las misiones internacionales y el cambio de rol de nuestras FAS en ellas han hecho que se incremente la importancia de la logística del combustible y la mejora de la eficiencia energética en bases y campamentos.

El incremento de la demanda energética debido al crecimiento de las economías emergentes y la dificultad para encontrar nuevos campos de petróleo convencional ha mantenido el precio del crudo y de los combustibles fósiles en general a un nivel elevado durante la última década. El nivel de precios, con una subida casi constante excepto

36 Cuadernos de Estrategia 166 Energía y Geoestrategia 201Instituto Español de Estudios Estratégicos.

en la brusca caída del año pasado, ha hecho que algunas tecnologías de extracción de hidrocarburos ya conocidas desde hace décadas fueran rentables. Esto, junto con un importante impulso político ha hecho que en varios países estas tecnologías han supuesto un cambio disruptivo en el sistema energético con implicaciones para la política de Defensa a nivel mundial. El impulso a la tecnología de "fracking" para la obtención de gas natural cambiando su mix energético de tal forma que el gas ha pasado a tener un papel básico en la generación de electricidad. También se han comenzado a explotar arenas bituminosas, una fuente de petróleo conocida pero cuya explotación es muy costosa.

La nueva capacidad de producción de crudo de EE.UU. y su independencia energética ha hecho que se reduzca la capacidad de presión de la OPEP y la importancia estratégica de Oriente Medio. Esta nueva política energética tendrá importantes efectos durante los próximos años en países exportadores (Rusia, Venezuela, Oriente Medio, algunos países de África) y en tradicionales importadores (Unión Europea, Japón, India, China).

Más allá de los combustibles fósiles no convencionales, el desarrollo de nuevos biocombustibles tiene importantes implicaciones geoestratégicas y operativas. Los biocombustibles de primera generación se han basado en cultivos que competían en recursos con cultivos alimenticios y su ciclo de vida tenía una importante huella de carbono. Desde el punto de vista de Defensa, estos biocombustibles además tenían unas características técnicas inferiores a las de los combustibles fósiles. Actualmente, se encuentra en desarrollo una segunda generación basada en cultivos no alimenticios biomasa de diversa procedencia, en la que el objetivo es romper la cadena de celulosa para mayor aprovechamiento energético.

En una fase más temprana de I+D se encuentran iniciativas basadas en bioingeniería y modificación genética de organismos como algas, para su aprovechamiento como fuente de biomasa, o de bacterias que sinteticen biocombustibles. Cabe destacar el reciente desarrollo que ha anunciado el Nocera Lab (Figura 15) de la Universidad de Harvard en el que a través de dos fases se ha podido realizar una fotólisis de agua para obtener hidrógeno, empleado junto con CO_2 en la segunda fase por una bacteria modificada (ralstonia eutropha) para sintetizar isopropanol.[37]

37 http://www.pnas.org/content/early/2015/02/06/1424872112.

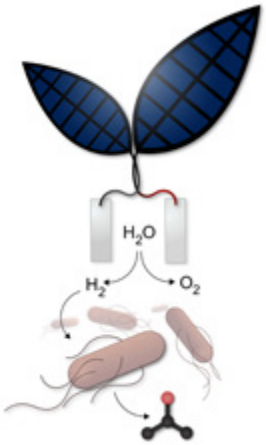


Figura 15. Concepto de hoja biónica desarrollada por Nocera Lab. Fuente: http://hms.harvard.edu/news/bionic-leaf.

Estas nuevas generaciones de biocombustibles pueden suponer un factor importante para mejorar la independencia energética de Europa, con un papel similar al de los combustibles fósiles no convencionales para Norteamérica.

En otro orden de cosas, la disponibilidad de energía es un factor clave en cualquier operación. A nivel logístico y operativo, el paradigma tradicional ha pasado por emplear combustibles líquidos, diésel y queroseno principalmente, como vector energético debido a su elevada densidad energética. Dicho combustible se emplea directamente en los sistemas de propulsión de plataformas o se transforma en electricidad mediante grupos electrógenos para alimentar todos los consumos de las bases: sistemas de comunicación, hospitales, iluminación, climatización, agua caliente, etc.

El cambio de tipología en las misiones, con un incremento de operaciones en las que nuestras FAS deben realizar tareas de ayuda humanitaria o como fuerzas de interposición en las que permanecen en bases fijas durante largo tiempo y en las que el mantenimiento de cadenas logísticas implica un elevado esfuerzo hacen que el paradigma tradicional suponga una importante barrera.

En este nivel se producirá un cambio a medio plazo a través de la transferencia de tecnologías de generación distribuida desarrolladas para el ámbito civil. Hasta ahora, la arquitectura de los sistemas de energía civil y militar han ido divergiendo, dado que el primero se ha basado en la creación de sistemas nacionales e incluso supranacionales de generación eléctrica a través de grandes centrales que envían la energía mediante costosas infraestructuras hasta centros de consumo alejados. No obstante, la preocupación por la eficiencia energética y el aprovechamiento de recursos energéticos in situ, junto con un desarrollo tecnológico importante en varios campos ha hecho que técnica y comercialmente sea viable crear redes de generación distribuida a nivel local. El desarrollo de redes inteligentes "smart grids" permite la conexión entre varias fuentes de energía, sistemas de consumo que puedan ser controlados mediante el internet de las cosas y sistemas flexibles de almacenamiento de energía.

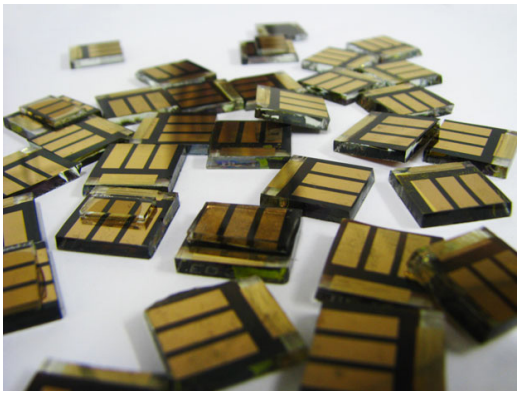


Figura 16. Perovkskitas. Fuente: Universidad de Oxford.

Para su uso en Defensa son de interés las tecnologías para el aprovechamiento de energías renovables, el desarrollo de células solares ligeras y flexibles que logren eficiencias superiores a las de las tecnologías comerciales actuales de paneles sobre vidrio. Destaca el salto en eficiencia que han logrado las células basadas en perovskitas (Figura 16) que han pasado de 3,8% a casi un 20%,[38] sistemas como la gasificación de residuos como en TGER[39] o el aprovechamiento de recursos renovables (eólica) o sistemas de back-up no convencionales (pilas de combustible).

Para la mejora de la eficiencia energética, el desarrollo de nuevos sistemas de climatización (activos y pasivos) y la integración de sistemas ya probados en el ámbito civil puede reducir el consumo energético en operaciones de forma drástica. Caben destacar experiencias como la Net Zero Energy Installations[40] del U.S. Army (Figura 17) y el NREL donde se ha logrado reducir el consumo energético un 25% en instalaciones en territorio nacional o el estudio *Smart and Green Energy (SAGE) for Base Camps*[41] (Figura 18) que estableció que mediante una combinación adecuada de tecnologías se podría reducir el consumo en bases en operaciones entre un 49 y un 84%.

38 http://spectrum.ieee.org/green-tech/solar/perovskite-is-the-new-black-in-the-solar-world.

39 http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallereferencia.aspx?referenciaID=37.

40 http://www.nrel.gov/defense/projects.html.

41 http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallereferencia.aspx?referenciaID=53.

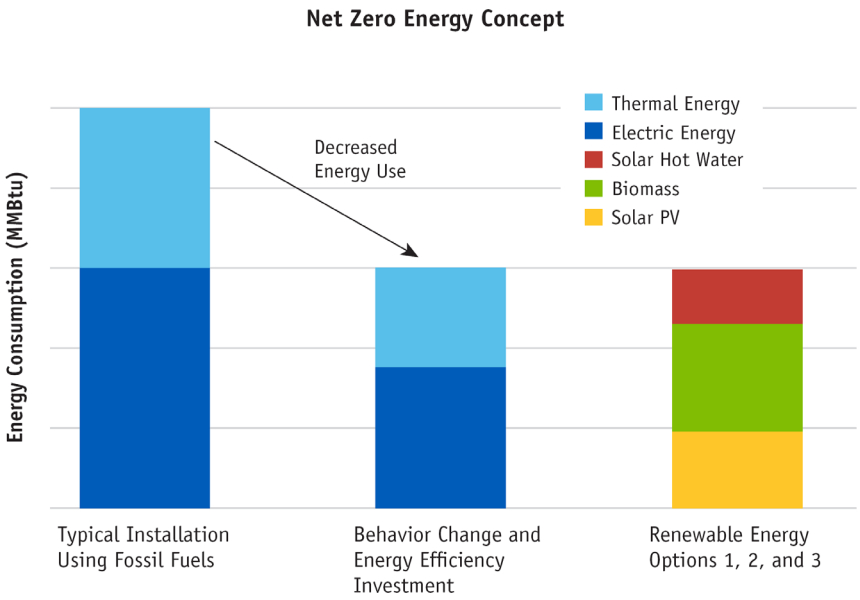


Figura 17 Concepto Net Zero Energy. Fuente: ARMY NET ZERO Energy Roadmap and Program Summary.

Figura 18. Molinos de viento y colectores solares. Fuente: http://www.monolithic.org/commercial/military-praises-south-industries-monolithic-dome-project.

CONCLUSIONES

Las tecnologías con efecto disruptivo han mostrado en multitud de ocasiones en la historia del hombre su poder transformacional y el mero de hecho de explotarlas ha supuesto marcar las diferencias entre las civilizaciones y esto es aún más reseñable cuando nos referimos al ámbito de las armas.

Pero no siempre estos procesos han sido eficientemente gestionados, habiendo sido en la mayoría de las ocasiones fruto del azar o de circunstancias concretas las que han llevado a un hallazgo que con carácter previo no fue estimado o suficientemente identificado en todas sus dimensiones.

Se manifiesta la necesidad de habilitar los mecanismos que propicien el florecimiento de tecnologías disruptivas, mediante el establecimiento de medidas adecuadas de financiación, ya que como se ha demostrado, pueden ser capaces de multiplicar en varios órdenes de magnitud la inversión efectuada, y de aportar un marcado factor diferenciador en contraste con otras estrategias de inversión más conservadoras. Pero esto sólo es posible si se implementan los instrumentos necesarios para el análisis, vigilancia, prospectiva, supervisión y control de las tecnologías potencialmente disruptivas y de las iniciativas de I+D y actividades en torno a las mismas. Para sacar esto adelante es necesario partir del desarrollo de una estrategia específica que sea capaz de explotar las oportunidades que éstas tecnologías brindan, y que ponga las bases adecuadas para los mecanismos e instrumentos de I+D antes mencionados.

BIBLIOGRAFÍA

Friedman,T. L. 199*The Lexus and the Olive Tree: Understanding Globalization.* New York: Random House.

Brimley, S., et al. Septiembre 201*Game Changers. Disruptive Technology and U.S. Defense Strategy.* Disruptive Defense Papers.

FitzGerald, B., et al. Junio 201*Creative Disruption Technology, Strategy and the Future of the Global Defense Industry.* Center for a New American Security.

Bower, J. L., Christensen, C. M. Enero-Febrero 199*Disruptive Technologies: Catching the Wave.* Harvard Business Review 73, no. 1: 43–53.

Martinage, R. 201*Toward a new offset strategy. Exploiting US long-term advantages to Restore US global power projection capability.* Center for Strategic and Budgetary and Assessments (CSBA).

Christensen, C. M. 199*The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail.* Boston, MA: Harvard Business School Press.

Riola, J. M. 201*La situación actual de las tecnologías de doble uso.* Cuadernos de Estrategia 169 Desarme y control de armamento en el siglo XXI: limitaciones al comercio y a las transferencias de tecnología. Capítulo CESEDEN. Instituto Español de Estudios Estratégicos

RTO-TR-SAS-062 AC/323(SAS-062)TP/25201*Assessment of Possible Disruptive Technologies for Defence and Security.* Final Report of Task Group 06

RTO-TR-SAS-082 AC/323(SAS-082)TP/42201 *Disruptive Technology Assessment Game – Evolution and Validation.* Final Report of Task Group 08

Riola, J.M., Díaz, J. J. 201*Vehículos no tripulados de ámbito naval.* Artículo de la publicación *Las tecnologías de doble uso: La investigación de Defensa como motor del desarrollo tecnológico.* CUD de San Javier.

Riola, J.M., Díaz, J. J. 201*Los sistemas de vigilancia competitiva*. Artículo de la publicación *Las tecnologías de doble uso: La trasferencia entre Fuerzas Armadas, Empresa y Universidad.* CUD de San Javier.

Riola, J. M. 201*La política de I+D+i de Defensa: Metas y retos tecnológicos*. Artículo de la publicación *Las tecnologías de doble uso: La investigación y el desarrollo al servicio de la sociedad civil y militar.* CUD de San Javier.

Evans, D. N. 200*Business Innovation and disruptive technology.* Prentice Hall.

Godet, M. 200Preface by Joseph F.Coates. Creating Futures. Scenario Planning as a Strategic Management Tool.

McKinsey Global Institute. 201.*Disruptive technologies: Advances that will transform life, business, and the global economy.*

Richard Slaughter, Chris Riedy. 199*The "state of play" in the futures field: a metascanning overview.* Foresight. Volume 11 Issue

Wheelwright, Steven C. 199*Note on Taguchi Methods for Improving Quality Through Design.* Harvard Business School Background Note 691-076.

Saaty, Thomas L. 200*Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World.* Pittsburgh, Pennsylvania: RWS Publications.

López, P. 200*Tecnologías Disruptivas: Mirando el futuro tecnológico Ministerio de Defensa.* Boletín de Observación Tecnológica en Defensa nº 2

García, D., López, P. 201*Jornadas sobre Tecnologías Disruptivas en la RTO.* Ministerio de Defensa. Boletín de Observación Tecnológica en Defensa nº 3

López, P. 201*Tecnologías Disruptivas: de la LoI a la EDA.* Ministerio de Defensa. Boletín de Observación Tecnológica en Defensa nº 3

Requejo, L. 201*Seminario sobre los resultados de proyectos JIP-FP y JIP-ICET de la EDA.* Boletín de Observación Tecnológica en Defensa nº 3

Riola, J. M. 200*Especial Las CapTechs de la Agencia Europea de Defensa*. Boletín de Observación Tecnológica en Defensa nº 2

Martínez, J. 201*Instituto Español de Estudios Estratégicos. Biomímesis en los entornos de Defensa y Seguridad.* Documento de investigación. Centro Universitario de la Defensa de Zaragoza.

Erwin, S. 201*Top 10 Disruptive Technologies for a New Era of Global Instability.* Report. National Defense Magazine.

Schilthuizen, S., Simonis, F. 200*Nanotechnology. Innovation opportunities for tomorrow's Defence.*

CAPÍTULO 2

TECNOLOGÍAS DISRUPTIVAS Y SU IMPACTO EN LA SEGURIDAD Y DEFENSA

Resumen

La aparición de tecnologías disruptivas ha sido una constante a lo largo de la historia militar, al ser inseparable de la historia general de la civilización. La aparición y desarrollo de las armas nucleares es expuesta como epítome de estas y su influencia en los niveles estratégico y operacional.

A continuación se examinan una serie de tecnologías: sistemas autónomos en las tres dimensiones del campo de batalla, empleo del grafeno, armas de energía dirigida y sistemas portátiles de generación de energía.

Mención destacada ha merecido el modelo estratégico de Offset, propugnado por los Estados Unidos como medio de mantener una superioridad tecnológica que asegure la de sus fuerzas armadas.

Como conclusión se apunta que el espacio cibernético puede aportar efectos disruptivos a las operaciones y la dificultad de controlar y gestionar el desarrollo tecnológico debido a la condición de "doble uso" de la mayoría de los avances.

Palabras clave

Tecnología Disruptiva, Historia Militar, Armas Nucleares, Estrategia, Nivel Operacional, Energía, Sistemas Autónomos, Grafeno

Abstract

The emergence of disruptive technologies has been a constant throughout military history, being an inseparable part from the general history of civilization. The emergence and development of nuclear weapons is exposed as the epitome of these and their influence on the strategic and operational levels.

Coming up next there is a number of technologies examined: autonomous systems in the three dimensions of the battlefield, use of graphene, directed energy weapons and portable power generation systems.

The Offset Strategic Model deserves a special mention; advocated by the United States as a means of maintaining a technological superiority that ensures that of its armed forces.

As a conclusion, it is noted that cyberspace can bring disruptive effects in operations and the difficulty of controlling and managing technological development due to the condition of "dual use" of most advances.

Keywords

Disruptive technology, military history, nuclear weapons, strategy, operational level, energy, autonomous systems, graphene.

INTRODUCCIÓN

Como cualquier actividad humana, los esfuerzos para asegurar la supervivencia de las sociedades frente a las amenazas con las que se enfrentan han sido influidos por la permanente evolución de la tecnología. Pequeñas mejoras han supuesto, en ocasiones, ventajas decisivas en el combate. El paso de la baqueta de madera a la de hierro dio a las armas de fuego individuales una seguridad de funcionamiento y una cadencia de tiro que les hizo definitivamente superiores a cualquier arma blanca. Hay que tener presente que a principios del siglo XVIII, en la Gran Guerra del Norte entre Suecia y Rusia (1700-1721), Carlos XII todavía alineaba unidades de piqueros.

Otras veces ha sido una aproximación novedosa a un problema la que ha supuesto una verdadera revolución. Hasta después de la Guerra de los Siete años (1756-63), el empleo de las armas de fuego era realizado en formaciones masivas para reducir aprovechar al máximo las pobres cualidades de alcance y precisión de la mosquetería de la época. La aparición de un cartucho que comprendía la bala, la pólvora y el fulminante en un solo módulo, junto con el mecanismo de alimentación trasero y un mecanismo de disparo totalmente interno revolucionaron el aspecto del combate terrestre a partir del segundo tercio del siglo XIX.

Los problemas persisten a través del tiempo. En los casos anteriores, el soldado de infantería debe mejorar tanto su capacidad individual de combate como su contribución a la unidad en que se encuadra; para lo cual debe no solo incrementar su letalidad sino, de forma simultánea, su capacidad de supervivencia. Lo verdaderamente importante en la resolución de problemas es como se aborda. Y cuando esa forma supone un cambio radical al enfoque con que se ha intentado hasta ese momento aparece la disrupción.[42]

La disrupción en el caso de la tecnología militar, puede implicar la necesidad de un cambio que muchas veces las sociedades no están dispuestas a pagar, porque supone afectar al núcleo mismo de su esencia.

La pólvora fue disruptiva en el campo de batalla y eficazmente usada por los turcos en el campo de batalla. Sin embargo el sistema de gobierno otomano impidió que se aprovecharan los sucesivos avances en la tecnología del armamento, que en un primer momento habían incorporado a su tren de asedio.

Las nuevas armas exigían formaciones de infantería cerradas que maximizasen los reducidos efectos de las armas de la época, y eso no era compatible con la distribución de los jinetes turcos como vigilantes depredadores de las poblaciones sometidos. En

42 Tecnologías Disruptivas. Mirando el futuro tecnológico. Patricia López Vicente. Boletín de Observación Tecnológica de la Defensa nº 25. Cuarto trimestre 2009.

menos de cien años, desde las guerras napoleónicas a las balcánicas, el imperio Turco fue barrido de Europa y no por falta de población movilizable. Las nuevas armas exigían masas cohesionadas que el sistema del "millet" no podía proporcionar, sino todo lo contrario al perpetuar un sistema de agravios y desniveles insalvables para la mayoría.

Ni siquiera los compromisos de mínimos al estilo del Imperio Austrohúngaro pudieron lograrse y eso vetó el aprovechamiento de una tecnología cuya aceptación se veía como una amenaza para la estructura del imperio.

En Europa Occidental, la persistencia en el empleo como arma del caballo, pese a la evidencia de la vulnerabilidad de las formaciones montadas estaba, en buena parte, fundada en la persistencia de unos esquemas sociales que veían en el caballo el ejemplo vivo de sus valores procedente de una tradición aristocrática que creían amenazada por la extensión del motor en el campo de batalla y la posible "vulgarización" del liderazgo, no solo militar sino social.

También el grado de complejidad en la organización social determina, en ocasiones, la capacidad de aceptación y extracción del máximo rendimiento de una tecnología. El nivel de alfabetización, el grado de iniciativa que se promueve en una determinada sociedad o, más recientemente, la extensión de las tecnologías de la información entre la población son factores que resultan determinantes a la hora de implantar y aprovechar cualquier mejora tecnológica, especialmente en el ámbito de la defensa.

Es revelador el ejemplo de la Unión Soviética, donde el ansia del estado por controlar las comunicaciones entre sus ciudadanos implicó un retraso en la introducción y difusión de la tecnología informática que supuso una dificultad creciente para los reclutas a los que había que enseñar el manejo de los ordenadores de la época desde sus rudimentos, mientras que sus equivalentes occidentales llegaban con una experiencia a través de las consolas y los primeros ordenadores personales, que les permitían dedicarse directamente a las aplicaciones militares.

UN EJEMPLO CLÁSICO, LAS ARMAS NUCLEARES

Introducción

Si a una tecnología se la puede caracterizar de disruptiva esta es la nuclear.

El aprovechamiento de la energía de los procesos de fusión y fisión del átomo supuso, en primer lugar, ir más allá de la evidencia sensible y establecer modelos de la

estructura más básica de la materia (proceso que todavía hoy no está culminado); crear un aparataje matemático que permitiese el establecimiento y desarrollo de los modelos físicos y llegar a la concreción material de todo lo anterior.

El resultado fue un arma de características revolucionarias. El nivel de destrucción que antes requería unos medios formidables se podía concentrar en una sola bomba transportada por un solo avión o navío o lanzada por una sola pieza artillera.

Los vectores de lanzamiento se multiplicaron. Al contrario de los explosivos convencionales, las distancias de seguridad de las tropas propias a la explosión, pasaron de contarse de decenas de metros a kilómetros. Esto implicaba que había que encontrar los medios de proyectar las cabezas de guerra nucleares lejos de las líneas propias pero con efectos que redundasen en las operaciones, lo que dio lugar a una doctrina específica para el apoyo de fuego con estas armas.

Las pruebas nucleares en el Atolón de Bikini entre 1946 y 1958 demostraron la extrema vulnerabilidad de cualquier flota ante las nuevas armas

Consecuencias Operacionales y Tácticas

Una de las primeras dificultades del empleo de las armas nucleares fue tratar de encuadrarlas en un determinado nivel de planeamiento y decisión de uso. Supuesto que se hubiese tomado la decisión, el Comandante de la unidad encargada de su aplicación sobre el enemigo había de afrontar no solo el empleo de una capacidad explosiva sin precedentes, con unos efectos mecánicos y térmicos que excedían la escala de la experiencia convencional, sino además aceptar las implicaciones de los efectos radioactivos.

Grandes extensiones de terreno quedarían contaminadas (La contaminación química en Flandes ha durado más de ochenta años) y esa contaminación era capaz de producir enfermedades durante lapsos de tiempo prolongados y por tanto la presencia o el simple cruce de áreas contaminadas exigían largos y costosos procesos de descontaminación. Por muy protegidas que pudiesen estar las dotaciones de los buques o las tripulaciones de los vehículos blindados al final, el empleo normal de los medios terrestres y navales requiere un mínimo de operaciones de mantenimiento que implica que para realizarse seguras hay que proceder a la reducción de los niveles de radiación a unos umbrales seguros.

El terreno quedaría conformado como un damero de zonas limpias y prohibidas, en el que la dificultad de ejecutar movimientos y planear sucesivas operaciones sería proporcional a la profusión en el empleo de armas nucleares.

Los primeros análisis de impacto táctico se hicieron sobre la experiencia de los procedimientos de combate soviéticos durante la Segunda Guerra Mundial. Las concentraciones de carros y artillería como paso previo a las masas de infantería que habían caracterizado las ofensivas finales soviéticas en Bielorrusia y Polonia constituirían a partir de ahora un blanco tan rentable que cualquier planificador militar consciente las tendría que evitar si se enfrentaba a la posibilidad de un ataque nuclear. Ello llevó a una parálisis a lo largo de las líneas fronterizas entre el Este y Oeste en la Guerra Fría en Europa.

La incapacidad de superar la concentración de medios en un espacio proporcionalmente reducido, que acarrearía unos niveles de bajas que empequeñecerían las más sangrientas batallas de la 1ª Guerra Mundial, mantuvo el estatus quo en Europa generación tras generación de carros de combate, piezas de artillería y vectores de lanzamiento, que ya no pudieron ofrecer alternativas creíbles de una supervivencia decisiva en el entorno nuclear.

Conceptualmente la situación tenía un cierto parecido con la Gran Guerra cuando la fase de guerra de trincheras sucedió a la de movimientos tras el fracaso del Plan Schlieffen en 191Un modelo táctico se enfrentaba a la imposibilidad de su desarrollo y la incapacidad de superar esta parálisis enquistaba una situación en el tiempo. Desde el inicio de la Guerra Fría hasta la caída de la Unión Soviética el "frente" no se movió ni un milímetro pero se ensayaron varias alternativas conceptuales (Air – Land Batlle, FOFA) destinadas a poner el énfasis en el combate contra la primera línea o las sucesivas que tenían que mantener el impulso ofensivo de esta.[43]

La sensación constante en las fuerzas occidentales de estar siendo superadas en número y calidad por el Pacto de Varsovia fue el hilo conductor de esta evolución conceptual que pretendía superar modelos a desgaste heredados de la Segunda Guerra Mundial.[44] Se trataba de encontrar modelos para combatir en inferioridad numérica y ganar.[45]

Nunca se sabrá si estos conceptos de empleo de las fuerzas terrestres de la OTAN hubiesen tenido éxito frente a una ofensiva del este. En todo caso hubiese implicado coordinar además de las fuerzas terrestres y aéreas el empleo de armas nucleares de corto alcance e intermedio, lo que hubiera supuesto un nivel de destrucción sin precedentes y que de forma prudente se prefirió evitar.

43 NATO'S Follow-on Force Attack (FOFA) Concept Past, Present and Future. LTC Michael J. Diver. Monografías US Army War College, Carlisle (Pennsylvania, USA) Julio 1990.

44 The Transformation of Europe's Armed Forces: From the Rhine to Afghanistan. Anthony King. Cambridge University Press. 2011.

45 Alternative Conventional Defense Postures in the European Theater. Vol 3. Hans Günter Brauch & Robert Kennedy. Taylor & Francis, Washington (USA) 1990.

Consecuencias Estratégicas

Si los militares afrontaban una serie de dilemas oportunidad/desventaja, en los niveles más elevados de los sistemas de toma de decisión, ya fueran democráticos o dictatoriales, las alternativas que se planteaban no eran menos complejas.

Una fue que los vectores de lanzamiento pasaron no solo de polimotores de hélice a bombarderos a reacción con una autonomía y unas prestaciones de vuelo que cada vez los hacían más difíciles de detectar y derribar;[46] otra que se introdujeron una serie de misiles basados en tierra o en plataformas aéreas o navales que daban un tiempo de reacción que pasó de horas a minutos.

La crisis de Cuba se originó precisamente porque el emplazamiento de los misiles soviéticos en la isla reducía prácticamente a cero la capacidad de alerta condenando a cualquier represalia a la inmediatez y la contundencia y a la dirección política a asumir el peso de decidir un Armagedón nuclear. Al contrario que en julio de 1914 la posibilidad de empleo inmediato por un lado carecía de las señales clásicas de alistamiento de las fuerzas, la consabida movilización general, la sola presencia de vectores de lanzamiento a una determinada distancia suponía un despliegue ofensivo tan inaceptable para Estados Unidos como la invasión de Bélgica para los británicos.

La crisis que se vivió entonces no deja de tener unos ribetes de hipocresía cuando se piensa que unos años después las clases de submarinos nucleares "Los Angeles" de los Estados Unidos y "Typhoon" soviéticos permitían una presencia constante y de difícil detección a distancias muy cortas de las costas "enemigas" respectivas sin despertar ninguna crisis diplomática. La posibilidad de un ataque "sorpresa" se materializó y la respuesta solo pudo ser la supervivencia de los medios nucleares propios y de los sistemas de mando y control, lo que originó el embrión de Internet.

La trascendencia de las decisiones pasó de afectar exclusivamente a los potenciales beligerantes a extenderse al conjunto del planeta. En un enfrentamiento termonuclear global no cabrían declaraciones de neutralidad y el efecto de un arma detonada a cientos de kilómetros podría ser fatal para un estado que sin participación alguna en los acontecimientos viera su producción de alimentos y sus acuíferos contaminados y a su población enferma.

En el plano humano, la experiencia de las catástrofes humanas vividas en las dos guerras mundiales precedentes sirvieron para que una generación de dirigentes que

46 El B- 29 que lanzó la bomba sobre Hiroshima podía llevar 9.000 Kg de bombas con una autonomía de 5.200 Km a una velocidad de crucero de 350 Km/h, mientras que un B – 52, de los años sesenta y setenta cargaba 31.500 Kg de armas con una autonomía de 7.120Km, pudiendo superar los 1.000 Km/h.

había combatido en al menos una y visto las consecuencias de ambas evitaran jugar a aprendices de brujo y se crearan sistemas de toma de decisiones que absolutamente centralizados.

Afortunadamente ninguna tecnología pudo romper el *impasse*, ni siquiera la Iniciativa de Defensa Estratégica lanzada por Reagan en 1983 logró materializar una capacidad creíble de detener un ataque masivo contra el territorio norteamericano, lanzados a una esgrima sin escudo el temor a una decisión sin ganancias, que supondría iniciar las operaciones nucleares, funcionó efectivamente durante la pervivencia del mundo bipolar.

Conclusión

La tecnología nuclear ha resultado disruptiva fundamentalmente no por sus efectos en el campo de batalla sino por el cambio en los modos de manejar el hecho bélico en el nivel político. La disuasión se tornaba invencible llegado a un punto de disponibilidad de armas, vectores y tecnología de guía. Ningún objetivo político ni militar era alcanzable si se producía el empleo en un sistema estratégico en el que las capacidades nucleares hubieran llegado a un cierto grado de desarrollo. Sin embargo queda la duda de que sucederá en un futuro con un sistema estratégico mundial con varios poseedores de estas armas, ubicados en entornos estratégicos distantes y con un número de cabezas o de vectores que no representen una amenaza de destrucción total para el conjunto de ese entorno. En estos entornos estratégicos regionales, la posibilidad de un empleo del arma nuclear con pérdidas aceptables aparece como una posibilidad, no porque la capacidad de destrucción no ejerza un saludable temor, sino porque siempre queda la esperanza de que sistemas de mando y control débiles y sociedades con tecnologías de la información relativamente poco extendidas puedan crear la esperanza de parálisis o desistimiento en el enemigo. Quizás Oriente Medio y el Subcontinente Indostánico sean los ejemplos más claros de lo anteriormente expuesto. Si a esto se suman pensamientos estratégicos con factores de análisis trascendentes a la existencia humana, la posibilidad de un uso de las armas nucleares puede estar repuntando peligrosamente.

TECNOLOGÍAS QUE PUEDEN AFECTAR A LAS OPERACIONES

Generalidades.

Si la disrupción se asocia a un cambio brusco, la historia militar está llena de *eslabones perdidos* y extinciones masivas. Está claro que los ejércitos y las armadas son hijos de las sociedades y el tiempo en el que se desarrollan y reflejan, como decía la Doctrina del Ejército de Tierra de 1980, "las virtudes de la raza", y la tecnología del entorno que los origina.

Evidentemente las mejoras de las tecnologías empleadas en el campo de batalla han sido en ocasiones determinantes en los resultados de los enfrentamientos, pero hay una prudencia, hija tanto del tradicional conservadurismo militar como de la prudencia frente a innovaciones no probadas, que ha hecho que la incorporación a las fuerzas armadas de las mejoras (y de algunas "peoras") se hayan introducido con lentitud, a veces catastrófica para los más retrasados.

Antes de formular críticas mirando hacia atrás por encima de la historia hay que tener en cuenta que las inversiones que se necesitan en recursos económicos y humanos para permitir la disrupción no siempre parecen que vayan a dar unos réditos que las justifiquen.

La propulsión a vapor, en sus orígenes, no era apta para su incorporación a los buques de línea, que siguieron manteniendo prudentemente las velas hasta el último tercio del siglo XIX. En este caso, además se suscitó un nuevo problema. Al contrario del viento, gratuito y generado de forma aleatoria pero espontánea por la naturaleza, la generación de vapor en los buques había de ser mantenida por medio de un combustible que ocupaba espacio en los buques y cuyo consumo implicaba la necesidad de una red de fuentes de aprovisionamiento. Hasta que el rendimiento y potencia de las máquinas y la disponibilidad de estaciones de carboneo en el área prevista de operaciones (para la Royal Navy el globo entero) no estuvieron dispuestos no se afianzó el cambio de propulsión.

No solo las sucesivas mejoras en alcance de las armas, velocidad de las plataformas terrestres o navales y su capacidad para incorporar armamento más diverso y eficaz. También los modos de mando y control han sido condicionados. Las tecnologías de las comunicaciones han ido posibilitando el mando y control eficaz hasta hacer innecesario el contacto visual y permitir el control global de las operaciones y la dilución de los niveles de mando. El nivel político puede hoy controlar las intervenciones de las pequeñas unidades que puedan tener resultados de carácter estratégico. El caso del presidente Obama siguiendo en directo el ataque a la residencia de Osama bin Laden

es una muestra de cómo han cambiado las tecnologías de la información la división de niveles de conducción de las operaciones.

Solo cabe hacer una reflexión. Bin Laden murió por impactos de bala de un arma que, posiblemente, no excediese en prestaciones a las que empuñasen los terroristas de Al Quaeda en sus acciones. Pero lo que permitió situar a los soldados norteamericanos en la ciudad pakistaní de Abbottabad y efectuar una "típica" acción de combate en población fue el empleo de una tecnología CIS puntera, que seguramente estaba siendo usada para aplicaciones civiles desde hacía tiempo. Esto nos lleva a que las tecnologías pueden producir un "efecto disruptivo en su empleo" aunque la tecnología que se haya empleado en su ejecución sea de uso común en otros campos o que tecnologías que por separado resultan conocidas pueden tener un efecto multiplicador en la eficacia de las capacidades militares. En general la tecnología informática ha supuesto un avance revolucionario en las capacidades de los sistemas de armas convencionales.

La Búsqueda de la Brecha. OFFSET

Hasta el presente se puede rastrear la simbiosis entre avances tecnológicos en los campos civiles y militares, pero es muy difícil afirmar que, por ejemplo en el caso del desarrollo de la física nuclear, nadie, ni científicos ni gobiernos estuviesen pensando en el aprovechamiento de la investigación como arma. Sin embargo, fue precisamente la explosión tecnológica que se produjo en los años cincuenta y la circunstancia estratégica de la guerra fría lo que condujo a que, como en las leyendas góticas, los alquimistas fueran recluidos en la torre por los nobles y se constituyesen en ambos bloques vastos programas de investigación científica aplicados a la defensa, con el objetivo decidido de hacer del conocimiento un arma que proporcionase la base de una decisiva superioridad sobre el enemigo.

En nuestros días, esta búsqueda consciente de "a la supremacía por la tecnología" tiene su reflejo en el programa OFFSET 3[47] de los estados Unidos. Se trata de mantener una serie de capacidades militares basadas en unas tecnologías que le permitan superar la actual situación, a la que se la compara con los peores momentos de la guerra fría en los que pareció que la Unión Soviética iba a tomar una sustancial delantera, primera con las armas nucleares y luego con las convencionales. Estados Unidos busca compensar con tecnología las reducciones en tamaño de sus Fuerzas Armadas que anuncian los sucesivos recortes. Hay que tener en cuenta que en los países desarrollados el personal al servicio de la administración, suele extender su coste más allá de su vida útil y de su esfera personal. Beneficios sociales a las familias y coste en pensiones convierten a

47 Toward a new Offset Strategy. Robert Martinage. Center for Strategic and Budgetary Assessments. 2014. http://csbaonline.org/search/?q=offset+&x=6&y=11.

cuerpos numerosos de la administración como las Fuerzas Armadas o las de Seguridad en elementos con un coste en personal muy elevado, con lo que cualquier reducción en su tamaño, gracias a la asunción de misiones por sistemas no humanos siempre resulta un alivio económico, ya que las máquinas no necesitan atención al final de su vida útil.

Pero no solo el personal consume recursos más allá de lo asumible, referido a los despliegues navales[48] los portaeronaves de cualquier envergadura se enfrentan a tecnologías A2/AD[49] sumamente baratas en relación con el coste de los buques que pueden situarlos en áreas desde las que sus sistemas aéreos embarcados no alcanzan los objetivos vitales del enemigo, lo que obliga a replantearse los sistemas de armas actuales si se quiere mantener una capacidad de disuasión.

En suma, Estados Unidos está apostando por la tecnología de sistemas no tripulados, de la capacidad de vuelo furtivo, del dominio del espacio submarino, la habilidad para integrar sistemas de ingeniería compleja y una red global de vigilancia y ataque pretende mantener dos opciones para ejercer la disuasión. Por una parte una más "clásica" basada en la capacidad de hacer inalcanzable los objetivos del enemigo y por otra, generada al calor de los adversarios asimétricos, una capacidad de destruir los objetivos sensibles del enemigo por ocultos y protegidos que se encuentren, en la inteligencia que se le va a llevar a intercambios inaceptables. Esto último resulta más que dudoso porque es necesario que dos adversarios compartan la misma escala de valoración de activos, especialmente si uno no es un actor estatal. Si las bajas humanas, por ejemplo, son aceptables en cualquier escala y categoría, para uno de los contendientes, la única opción es la aniquilación física, cosa harto improbable de conseguir.

SISTEMAS AUTÓNOMOS EN EL CAMPO DE BATALLA

Generalidades

Desde un plano puramente teórico, la relación entre hombre y máquina puede ser de lo más variada, según se considere.[50]

48 http://thediplomat.com/2015/03/what-can-the-middle-ages-teach-us-about-us-naval-strategy/

49 Anti - Access/ Anti - Denial

50 An Introduction to Autonomy in Weapon Systems, Paul Scharre & Michael C Horowitz. Center for a New American Security, February 2015

- La relación de mando y control entre el hombre y la máquina.
- La complejidad de la máquina
- El tipo de decisión que se ha automatizado.

Siendo cada uno de ellos independiente de los demás. Lo más importante es que la tecnología avanza hacia sistemas en los cuales el hombre está cada vez más ausente de cualquier tipo de decisión que toma la máquina. Las armas y los sistemas que sin intervención humana cada vez son más frecuentes en el campo de batalla no solo toman decisiones, guían las que toman los humanos.

Hasta nuestro siglo las mejoras en la tecnología siempre supusieron una intervención humana. En vez de cabalgar sobre caballos se avanzaba hacia el enemigo en un carro de combate y en vez de subir a las jarcias las dotaciones se afanaban ante consolas llenas de indicadores de todo tipo. El rendimiento de la acción humana quedaba multiplicado sin duda.

Y aquí aparece el matiz más importante. Para conseguir niveles de destrucción similares cada vez se han ido necesitando menos intervención humana tanto de índole física como intelectual. Sin embargo una característica del siglo XX ha sido la aparición de sistemas automáticos, capaces de emplear programas cada vez más perfeccionados, para efectuar tareas en el campo de batalla que hasta entonces estaban encomendadas a la unión del hombre y la máquina. La vigilancia del campo de batalla está cada vez más en manos de sistemas sobre plataformas, principalmente aéreas, que independientemente de la intervención humana, son capaces de detectar la presencia elementos hostiles de acuerdo con el tipo de operación al que sirven y de enviar al centro de procesos de información un flujo de datos cada vez más preciso.

Hay que tener en cuenta que cuando se habla de sistemas autónomos no se debe de pensar exclusivamente en las plataformas que proporcionan la movilidad y que pueden estar, mediante los algoritmos de gestión de movilidad correspondientes, desvinculadas de la intervención humana, si no de los sistemas de adquisición o intervención de cualquier tipo que aquellas incorporen y su capacidad de conexión a las redes de datos propias.

El resultado es que la miniaturización, la nanotecnología y los desarrollos de software forman un todo indisociable que proporcionan la capacidad final al sistema.

No solo es que un UAV[51] permita el sobrevuelo sin riesgo para el personal, es que los sistemas de detección y reconocimiento que incorpora le permiten más precisión que al operador humano y una mayor velocidad y capacidad de adquisición de los mismos. A su vez los datos son procesados y almacenados de forma automática, eliminando tareas repetitivas que pueden originar errores, permitiendo una rapidez en el proceso

51 Unmanned Aerial Vehicle.

de toma de decisiones que está cambiando la estructura de toma de decisiones a todos los niveles al eliminar la necesidad de escalones intermedios y poner incluso al mando de nivel político con la realidad del campo de batalla y la responsabilidad de decisiones de índole táctica que van a tener repercusiones estratégicas.

Esto, a su vez, ha generado nuevas vulnerabilidades de orden tecnológico. La lucha en el ciberespacio se puede llevar a la captura, supresión de información o incluso la inserción de datos falsos en los sistemas de vigilancia autónomos. La República Islámica de Irán ha sido capaz de logros puntuales pero notorios en la lucha contra la vigilancia israelí en el sur del Líbano.

Un desarrollo más lento están teniendo los sistemas autónomos que operan en el mar, tanto sobre vehículos aéreos (el primer despegue de un UAV desde un portaaviones no se realizó hasta noviembre de 2013 desde el USS Theodore Roosevelt) como marítimos, en superficie o sumergibles, proporciona a cualquier buque unas posibilidades de detección temprana del enemigo y el seguimiento de cualquier actividad potencialmente hostil en todas las dimensiones y a unas distancias que hasta ahora requerían el empleo de medios aéreos que condicionaban el diseño y desplazamiento de los buques. Menor tamaño y mayor capacidad de ataque y supervivencia son las características que los medios autónomos ofrecen en el ámbito naval.

Mención aparte tienen los sistemas de detección y reconocimiento posicionados en el lecho marino de forma puntual y que permiten la obtención de información sobre los movimientos navales enemigos, especialmente de submarinos.

Es en los vehículos terrestres donde las dificultades son más notorias para un sistema no tripulado debido a que el medio ofrece un número de obstáculos más diversos y con mayor dificultad de ser sorteados. Por otra parte, muchas veces la capacidad de adquisición en sistemas basados en tierra está limitada por la línea de visión directa, lo que hace que el vehículo tenga que internarse hacia el enemigo en unas condiciones de movilidad que no garantizan su supervivencia y hacen posible su captura, con la consiguiente vulnerabilidad.

Esto ha hecho que se haya trabajado más en sistema que trabajan "dentro de las propias líneas" como porteadores automatizados de cargas pesadas y elementos de seguridad de instalaciones, ya que los requerimientos de supervivencia son menores.

Los sistemas no tripulados permiten, por otra parte, minimizar el impacto de la acción enemiga en la opinión pública. Si un sistema no tripulado, automatizado o no, es destruido o capturado hay consecuencias militares, pero es difícil que los medios recojan el hecho, e incluso si lo hacen, que el impacto en la opinión pública fuese comparable al que supondría una baja humana.

Esto hace que, en situaciones donde la probabilidad de bajas propias sea muy elevada, el empleo de sistemas automáticos o remotos sea normal. El empleo sistemático de drones por Israel en el sur del Líbano, pese a las consecuencias que ya se han expuesto,

no es comparable a la posibilidad de un derribo y la captura de un piloto por parte de Hizbulá, con las consecuencias que las exigencias para su canje tendrían en la política israelí.

En el empleo de estos sistemas como recolectores de información siempre aparece el límite de la interpretación de la misma. Si bien los sistemas basados en longitudes de onda distintas de las del espectro visible dan una mayor capacidad de superar las limitaciones de las capacidades humanas, hay que tener en cuenta que antes o después la intervención humana se va a producir.

Si se dejan decisiones susceptibles de estar recogidas en reglas de enfrentamiento, como la posibilidad del uso de las armas, en sistemas no humanos la posibilidad de error, y por consiguiente de bajas propias o de daños colaterales y ambos casos tiene un impacto directo en las operaciones.

Sin embargo los sistemas automáticos de defensa, que ante la detección de una amenaza real o potencial (ser simplemente adquiridos por un sistema de vigilancia o identificación reconocido como enemigo) desencadenan una respuesta, maniobra evasiva o acción de sistemas de armas, son fundamentales en la aviación de combate actual y pueden ser usados con facilidad en buques y vehículos terrestre. Estos sistemas de "decisión automática" constituyen una parte fundamental de la capacidad de supervivencia de las plataformas autónomas.

UAVs

Si en el campo de los sistemas autónomos caben numerosas especulaciones sobre el futuro, los UAVs suponen una acreditada realidad. Las imágenes en la televisión de ataques a objetivos de tierra con municiones de precisión desde UAVs nos muestran como sus pilotos ven el campo de batalla. La misma percepción del riesgo físico tiene uno de estos pilotos que el espectador en su casa. Incluso cuando se llegue al combate aire – aire entre sistemas remotos (cosa que solo es cuestión de tiempo y oportunidad) la necesidad de cualificación de vuelo, que hoy se mantiene en muchos países similar para cualquier tipo de pilotaje de aeronaves de combate, disminuirá sensiblemente para los UAVs.

De forma similar a como el caballero tardó en desaparecer por la presión social a su favor, el piloto de combate como élite de las fuerzas armadas en cuanto a requerimientos físicos y psíquicos que justifica una inversión en formación y su proyección de carrera dentro de las fuerzas armadas se mantendrá durante el tiempo que los desarrollos en sistemas de vuelos con pilotaje remoto no desbanquen definitivamente, al menos en caza y ataque, a los sistemas pilotados.

Un aspecto significativo a tener en cuenta son los costes. Estos pueden desglosarse en costes de construcción, mantenimiento y adiestramiento. En cualquier caso, la broma norteamericana sobre el avión F-xteen que sería usado en días alternos por los diferentes servicios dado que su coste impediría su fabricación en serie, pudiera tener su contestación en la reducción de costes que supondrían unas capacidades aéreas basadas en sistemas no tripulados. Piénsese solamente en que las capacidades de reconocimiento que los mini – UAVs han proporcionado a las pequeñas unidades de infantería evitan el empleo de medios blindados muchos más caros, no solo de adquirir sino de mantener a lo largo de su vida útil.

No solo para países de tamaño medio como el nuestro, sino incluso para grandes potencia, el abaratamiento de costes, incluidos los de enseñanza y adiestramiento es fundamental en cualquier escenario económico. Evidentemente el desarrollo actual no permite el paso directo de una fuerza basada en sistemas pilotados a otra de sistemas guiados desde tierra. Como en otras tecnologías ambos tipos de aeronaves han de solaparse y generar sinergias entre sus capacidades. Los sistemas no pilotados proporcionan un grado de proyectabilidad y capacidad de intrusión muy elevada, pero su carga útil es todavía muy limitada comparada con un avión tripulado.

Su supervivencia, y en general toda su eficacia operativa, está basada en su furtividad, pero eso le resta, hasta el presente, las capacidades aire – aire y de empleo de municiones pesadas. El misil "Hellfire" característico de los "Predator" norteamericanos tiene una buena capacidad para ataques sobre vehículos incluso con un alto blindaje y sobre edificaciones. Pero es dudoso que su empleo contra un despliegue convencional de infantería a pie pudiera tener la efectividad de una bomba de caída libre y peso superior a los 200 Kg con la que se consiguen efectos sobre formaciones muy diluidas. Una célula terrorista en un vehículo circulando por una carretera puede ser un objetivo rentable para un ataque como los que se han realizado en la frontera entre Pakistán y Afganistán o en Yemen. Tratar de detener el avance de un batallón motorizado con la misma capacidad de ataque exigiría un elevado número de UAVs, lo que los convertiría en vulnerables a una defensa antiaérea que en el caso de los terroristas no existe, o en blancos para aparatos de ala fija o rotatoria con capacidad aire - aire.

En definitiva, que los UAVs irán tomando, de forma lenta pero segura, el lugar de honor en algunas capacidades de las fuerzas aéreas pero a medio plazo.

Sistemas Autónomos y la Seguridad Nacional

La demografía española, la situación económica, incluso en escenarios de bonanza, y las características del sistema político hacen que un conflicto armado en nuestra vecindad, con participación más o menos intensa, o no, de nuestras Fuerzas Armadas sea la opción más peligrosa para nuestra seguridad. El volumen decreciente de gasto

dedicado a Defensa hace que haya que maximizar las inversiones buscando en las tecnologías más avanzadas la consecución de una brecha tecnológica con nuestros posibles adversarios, o los contendientes de cualquier conflicto posible en nuestro entorno geoestratégico, que permita, si no la disuasión, al menos una respuesta eficaz y minimizar las pérdidas de todo tipo en las fuerzas propias, permitiendo su empleo durante el mayor tiempo con las máximas capacidades.

Está claro que en esa doble búsqueda, minimización de pérdidas, humanas y materiales y maximización de efectos las tecnologías disruptivas, y en concreto las plataformas autónomas aportan soluciones reales.

Este hecho supone una disuasión implícita, no afecta a capacidades de respuesta pero disminuye el factor opinión pública que podría hacer pensar a un posible enemigo que no se le respondería con el poder militar por miedo a las bajas propias o a posibles daños colaterales. Además, hay que tener en cuenta que la capacidad de permanencia sobre un área supera a la de cualquier sistema tripulado al evitar factores limitativos de los sistemas biológicos (alimentación, descanso, disminución de la atención). Esto añade un componente adicional de disuasión, no solo entre los actores estratégicos nacionales, sino también entre los grupos terroristas o criminales que ven como la vigilancia se extiende sobre zonas y tiempos que antes permitían unos cálculos de coste/ beneficio más favorables a la hora de ejecutar acciones contrarias a los interese españoles.

Respecto a la lucha contra el crimen organizado las plataformas autónomas, cualquiera que sea el tipo de sensores que incorporen, problemas legales aparte, proporcionan una capacidad de vigilancia sobre personas y lugares que proporcionan una cantidad notable de evidencias, tanto para preparar y apoyar la intervención de agentes humanos como para la recolección de evidencias de uso en procesos judiciales. Se evita de esta manera vigilancias humanas con la consiguiente disminución de agentes empleados en tareas rutinarias evitando su identificación por elementos criminales.

Por otra parte, el mantener sometida a vigilancia y gestión de inteligencia a zonas que requieren por su extensión o características físicas o humanas (difícil acceso o capas de población que apoyan el delito como alternativa a una ocupación regular) grandes efectivos de seguridad disminuye los espacios de impunidad obligando a los grupos criminales a desarrollar su actividad en zonas o con procedimientos más fácilmente detectables. Las fronteras terrestres de las Ciudades Autónomas de Ceuta y Melilla y las aguas del Estrecho de Gibraltar así como las áreas de tránsito de las embarcaciones que transportan inmigrantes ilegales hacia las costas del sur de la Península son un campo de actuación donde estos sistemas pueden demostrar una alta rentabilidad.

En este caso, además, se estarían afrontando las amenazas de los flujos migratorios irregulares y de la vulnerabilidad del espacio marítimo. En la lucha contra la proliferación de armas de destrucción masiva la capacidad de mantener vigilancias prolongadas permite la monitorización efectiva de posibles emplazamientos de fabricación así como

rutas de acceso de materiales que sirvan de base a su fabricación. No solo mediante plataformas autónomas, sino mediante una extensa red de sensores inatendidos que proporcionan desde el mundo real o el virtual un flujo constante de datos.

SISTEMAS DE ENERGÍA PROYECTABLES

El desarrollo tecnológico implica el abastecimiento constante de energía que alimente los sistemas que se van desarrollando. Si bien en un principio las fuentes de energía eran tomadas directamente de la naturaleza, proteínas animales y vegetales y la fuerza del viento y del agua, así como la combustión de vegetales, a partir del desarrollo de los motores de combustión externa que generaban la vaporización de agua para aprovechar su fuerza expansiva, se generó un doble problema, la obtención de materiales susceptibles de generar energía y asegurar su abastecimiento para las fuerzas armadas, que en el caso de potencias con intereses globales generaba, a su vez, una geopolítica de los recursos.

Sin embargo, hasta fechas tan próximas como la I Guerra Mundial, el que sofocarían a un abastecimiento que más exigió del sistema de transportes británico (en cuanto a volumen se refiere) fue el forraje para mantener a los caballos que proporcionaban la movilidad a la Fuerza Expedicionaria en Francia. Apenas veinticinco años más tarde, el pienso y la avena eran anecdóticos en los ejércitos aliados y un flujo constante de derivados del petróleo mantenía en marcha las ofensivas que sofocarían a un Eje que mantuvo hasta el final la mayor parte de sus unidades con tracción hipomóvil.

No solo las fuerzas terrestres, las aéreas y las navales dependen para su empleo de un abastecimiento constante de combustible y no solo para volar o navegar. Todos los sistemas de mantenimiento y control de los espacios aéreo y marítimo, así como las instalaciones de vida y servicio para las dotaciones necesitan una energía segura y constante capaz de convertirse, básicamente en un fluido eléctrico seguro para aplicaciones que van desde la iluminación a la operación de sistemas informáticos que requieren una gran calidad en la estabilidad de la corriente.

Como normalmente las zonas de conflicto se encuentran alejadas de los suministros regulares o, por efecto del mismo este se ha visto suspendido, la capacidad de proporcionar desde comodidad al personal hasta permitir que los sistemas portátiles que funcionan con baterías recargables se basa en la posibilidad de mantener fuentes de energía seguras en su operación, defendibles y proyectables.

Una alternativa son sistemas basados en el aprovechamiento de energías renovables, eólicas y solar, que ya han sido probados por los norteamericanos en Irak y Afganistán, pero que adolecen de los mismos problemas que las instalaciones en territorio nacional, cuando más se les necesita está nublado o no hace viento. Sin embargo cuando se piensa que en 2007 para abastecer a las fuerzas en Irak se necesitaban 3369006 litros

de combustible (8900 galones) diarios la búsqueda de soluciones a la vulnerabilidad que supone mantener una red de distribución basada en cisternas (rigidez de las líneas de comunicaciones que facilitan la planificación de ataques y facilidad de conseguir grandes daños con pocos medios) acepta soluciones complejas, como las estaciones de generación híbridas con capacidad de almacenamiento.[52]

No se trata de eliminar la dependencia de los despliegues operativos de los combustibles fósiles, al menos a corto y medio plazo, sino de permitir que pequeñas unidades, sistemas autónomos o el combatiente aislado considerado como un sistema de armas pueda acceder a una fuente de energía que le permita la operación de los sistemas "no de propulsión" necesarios para el cumplimiento de su misión.

Pensemos en los sistemas de reconocimiento facial y de trazas de explosivos que permiten mejorar la seguridad de una instalación fija. El conjunto integrado más su conexión a un posible sistema autónomo de identificación y evaluación de la amenaza mediante los datos enviados por los dos primeros debe funcionar constantemente, a veces en zonas de difícil abastecimiento combustible tradicional y así minimizar la amenaza de ataques suicidas. Un "mix" adecuado de generación y almacenamiento de energía se revela vital en este caso.

Cualquier sistema de almacenamiento, por muy mejorado que esté, llega un momento en que necesita una recarga. Los sistemas portátiles basados en generadores eólicos/ solares, junto con los generadores basados en las pilas de combustible pueden proporcionar la combinación de movilidad y nivel de prestaciones necesarios para situaciones de alta movilidad.

Alimentar en combate sistemas de puntería integrados para armas individuales con capacidad día / noche, posicionamiento y dirección de tiro para armas colectivas de infantería y sistemas de vigilancia del campo de batalla puede ser un reto en operaciones prolongadas, teniendo en cuenta que los fallos de alimentación pueden hacer desaparecer la brecha tecnológica que los sistemas anteriormente citados proporcionan a sus poseedores, muchas veces en inferioridad numérica tanto de efectivos como de armas individuales y que necesitan mantener una superioridad en prestaciones operativas para cumplir la misión con garantías de supervivencia.

52 Battlefield Energy. Breanne Wagner. National Defense Magazine. Abril 2007.

APLICACIONES MILITARES DEL GRAFENO[53]

Desde su descubrimiento en 2004 por Andréy Gueim y Konstantín Novosiólov en la Universidad de Manchester, el grafeno ha generado grandes expectativas que todavía no se han sustanciado en desarrollos concretos.

Está claro que su estructura molecular en una sola capa de átomos de carbono le confiere unas capacidades extraordinarias en cuanto a conductividad eléctrica, resistencia mecánica, conductividad del calor o elasticidad. Sin embargo, esa misma característica de la bidimensionalidad no le permite una existencia independiente, necesita el "maridaje" con otros elementos que permiten, formando materiales compuestos, su aprovechamiento industrial. Quizás el único aprovechamiento como material puro sea el de aditivo para combustibles, que ha permitido una mejora de las velocidades desarrolladas por aviones supersónicos y del rendimiento de motores diésel.

Existen otras aplicaciones como su introducción en fibras sintéticas para conseguir protecciones individuales de gran resistencia balística con un peso muy reducido, así como su posible uso en blindajes compuestos, si bien las expectativas que se pusieron en su día en los nanotubos de carbono no se han plasmado en realidades comerciales. Uniéndolo con lo anteriormente dicho sobre energía en el campo de batalla, su empleo como componente de baterías de muy larga duración puede hacer que el rendimiento de sistemas de generación de energía proyectables aumente al hacer que las mismas prestaciones proporcionen una mayor autonomía a los sistemas que abastece.

Una aplicación que puede ser importante, tanto como centro de un sistema de adquisición y reconocimiento aislado como formando parte de un sistema de armas más complejo es la sensibilidad a la luz del grafeno, que mejora exponencialmente los sistemas de adquisición y localización en cualquier gama del espectro, desde la luz visible a la infrarroja.

Si consideramos la generación de energía para los sistemas de reconocimiento y adquisición que equipan a los vehículos no pilotados, la reducción del combustible dedicado a hacerlos funcionar es fundamental para mejorar la autonomía del vehículo y, si es posible, aumentar la carga útil, con lo que la reducción de consumo en sistemas electrónicos que produce la excepcional capacidad de conductividad del grafeno será una de las mejoras que aportará.

53 Propiedades y aplicaciones del grafeno. Monografías del Sistema de Observación y prospectiva tecnológica. Ministerio de Defensa. 2013.

Si combinamos altos rendimientos energéticos del grafeno con la autonomía de las pilas de combustibles[54] se pueden obtener rendimientos muy elevados en cuanto a información / gasto de energía.

ARMAS DE ENERGÍA DIRIGIDA

Desde que H.G. Wells incorporó el "rayo calórico" a la panoplia de los marcianos en la "Guerra de los Mundos", el imaginario de las armas en la ciencia ficción se ha ido poblando de rayos mortales capaces incluso de desintegrar sus objetivos.

De forma más real, las armas de energía dirigida se están extendiendo en una serie de aplicaciones incipientes, basadas en una tecnología láser cada vez más asentada en todos los órdenes de la vida. Desde la luminotecnia de espectáculos musicales a bisturíes de la máxima precisión para la cirugía ocular, pasando por los dispositivos de lectura óptica de datos, el láser nos acompaña en la vida cotidiana, pero también va a ser la base armas cada vez más eficaces en todas las dimensiones del campo de batalla.

Un arma de energía dirigida[55] emite energía en una dirección determinada sin emplear ningún proyectil. La energía se transfiere directamente a un objetivo para conseguir un efecto determinado. Básicamente, estos efectos pueden ser no letales o letales. Desde un punto de vista técnico, la energía puede ser de diversos tipos:

- La radiación electromagnética, de láser o máser.
- Las partículas con masa, en rayos de partículas.
- Sonido en armas sónicas.

Armas láser podría tener varias ventajas principales sobre armamento convencional:

- Los laser viajan a la velocidad de la luz, por lo que no hay necesidad de compensar el movimiento del blanco cuando se dispara a través de largas distancias. En consecuencia, evadir un láser dirigido con precisión después de que ha sido disparado es imposible. Esto confiere una precisión y una fiabilidad de hacer blanco al primer disparo muy superiores a las armas que emplean proyectiles.
- Debido a la altísima velocidad de la luz es sólo ligeramente afectado por la gravedad, por lo que la proyección de largo alcance requiere poca compensación, al contrario que por ejemplo la artillería convencional que a partir de determinados

54 El UAV Ion Tiger de la marina de los estados unidos, de 13,81 Kg de peso, consiguió en 2009 volar durante 23 horas y 17 minutos con un motor alimentado por célula de hidrógeno.

55 http://docsetools.com/articulos-enciclopedicos/article_87425.html.

alcances requiere corrección por la fuerza de Coriolis. Otros aspectos, como la velocidad del viento no necesitan la introducción de correcciones en la mayoría de veces, a menos que se dispare a través de materia con alto poder de absorción.

- Los láseres pueden cambiar el efecto, variando la superficie sobre la que se aplica la energía, permitiendo una variedad de efectos que en las armas convencionales exige una planificación previa combinando cargas y proyectiles,
- Si la fuente de energía es suficiente, un arma de energía se puede considerar dotada de munición ilimitada. Lo que supone el final de una limitación logística tradicional, pero la aparición de una nueva, con lo que lo hablado anteriormente sobre los sistemas proyectables de energía cobra una importancia aún mayor. Ya no se está dilucidando sobre la capacidad de recargar sistemas individuales, ahora puede ser una cuestión de la operación de sistemas principales de armas.
- El retroceso, lógicamente pensando en sistemas equilibradores para sistemas pesados y no en armas individuales, es casi nulo lo que aligera y facilita los montajes en cualquier plataforma.
- El radio de acción de un arma láser puede ser mucho más grande que el de un arma balística, dependiendo de las condiciones atmosféricas y el nivel de potencia.
- Los rayos láser no generan sonido o la luz que detecten la situación del arma.

Un problema importante con armas láser son sus altos requerimientos de energía eléctrica. Los métodos actuales de almacenamiento, conducción, transformación, y dirigir la energía no son suficientes para producir un arma de mano conveniente. Los láseres existentes desperdician mucha energía en forma de calor, que requiere un equipo de refrigeración aún voluminoso para evitar daños sobrecalentamiento. La refrigeración por aire podría producir un retraso inaceptable entre disparos. Estos problemas, que limitan severamente práctico arma laser en la actualidad, podrían ser compensados por:

- Superconductores eficientes a alta temperatura, para hacer el arma más eficiente.
- Mejor rendimiento almacenamiento/generación. Parte de la energía se podría utilizar para enfriar el dispositivo.

Para todo lo anterior las propiedades del grafeno pueden ser una solución práctica, aunque no inmediata.

Como conclusiones operativas, el empleo de estos sistemas sería contra armas con sistema de guía de cualquier tipo y a la mayor distancia posible. Lo cierto es que no solo la detonación prematura de las cargas sino la destrucción de los sistemas de guiado puede ser una función a desarrollar eficazmente por los haces dirigidos.

El peso y volumen que implican los sistemas de alimentación y refrigeración hacen que, por ahora, solo sistemas navales sean capaces de albergar este tipo de armas con posibilidad de movimiento. El resto de los desarrollos están basados en instalaciones fijas terrestres, lo que supone tanto una limitación para su empleo como una vulnerabilidad muy elevada frente a sistemas aéreos enemigos.

De cualquier forma, a pesar de todas las investigaciones en marcha y de algunos éxitos en el campo de las armas no letales y los intentos de integrarlas en sistemas más completos como el Iron Dome israelí, las armas de energías dirigidas tardarán aún un tiempo en incorporarse a los sistemas plenamente operativos.

CONCLUSIONES

El efecto disruptivo, entendido como una forma absolutamente nueva de solucionar un problema militar a través de una positiva ventaja en el campo de batalla, no solo es una consecuencia directa de la posesión de una tecnología. La sociedad que incorpora una tecnología tiene que estar capacitada para los cambios que esa tecnología puede implicar. Situaciones de poder y privilegio pueden verse amenazadas o capas amplias de la población verse forzadas a una redefinición de su papel, a veces con cambios a peor a corto plazo.

La disrupción ha tenido un proceso tradicional de serendipia. A partir de la Segunda Guerra Mundial, empezando con los esfuerzos desesperados del Tercer Reich por encontrar armas milagrosas que evitaran una derrota catastrófica, la búsqueda de una brecha tecnológica decisiva ha ocupado recursos de todo tipo de los principales actores estratégicos.

La búsqueda de la disrupción ha traído consecuencias relevantes no solo en el campo de la aplicación al campo de batalla de determinados avances tecnológicos. Han aparecido nuevas dimensiones en el campo de batalla que se ha trasladado al dominio virtual y desde las armas nucleares al combate en el ciberespacio conceptos como disuasión han sufrido una transformación, si no en su formulación, si en su manejo en los niveles más elevados de la decisión.

Conceptos como los de ataque y defensa que tienen una expresión más o menos clara y estable en el dominio físico han quedado diluidos en el espacio cibernético. La necesidad de obtener el dominio de espacios no físicos ha hecho que el valor de muchos sistemas de armas empiece a ser considerado a partir del dominio de espacios de batalla no físicos, esto lleva a que para ejercer la disuasión no haga falta una carrera constante en la construcción de acorazados como a principios del siglo XX, carros de combate o aviones como en los años treinta del pasado siglo o cabezas nucleares.

La superioridad en el espacio cibernético puede marcar una barrera efectiva contra las aspiraciones de cualquier enemigo sea estatal o no, pero también concede a los actores no estatales, por modestos que sean, unas capacidades de influencia global que hasta ahora no tenían.

Para un país con la posición estratégica de España, con sus condicionantes de población y entorno estratégico mantener una superioridad tecnológica respecto a las amenazas de actores estratégicos estatales o no, e incluso frente a amenazas de carácter económico o no humanas es vital. La primera capacidad militar a que debe aspirar nuestro país es la de investigación en tecnología identificadas como potencialmente disruptivas. Habida cuenta de la capacidad de doble uso de estas tecnologías el retorno económico está asegurado y la inversión en seguridad siempre da los mejores dividendos.

De lo que no cabe duda es que, dado ese nivel de doble uso creciente de la tecnología y la actuación de actores no estatales tanto como actores estratégicos principales como "externalizados", como en el caso de los piratas informáticos, la posibilidad de que nuestros potenciales enemigos sean los que creen una brecha tecnológica a su favor es creciente y puede constituir un lastre estratégico del que sea difícil librarse.

BIBLIOGRAFÍA

Paret, Peter. *Creadores de la Estrategia Moderna* . Madrid: Ministerio de Defensa, 1992. 8478231803

Freedman, Lawrence. *La evolución de la estrategia nuclear.* Madrid : Ministerio de Defensa, 1992. 8478232249.

Headrick, Daniel R. *El Poder y el Imperio*. Barcelona: Crítica, 2011. 9788498921823.

López Vicente, Patricia. *Tecnologías Disruptiva. Mirando el futuro tecnológico*. Madrid. Ministerio de Defensa. Boletín de Observación Tecnológica de la Defensa nº 25. Cuarto trimester 2009.

Diver, Michael J, LTC US Army. *NATO'S Follow-on Force Attack (FOFA) Concept Past, Present and Future.* Monografías US Army War College, Carlisle (Pennsylvania, USA) Julio 1990.

King, Anthony. *The Transformation of Europe's Armed Forces: From the Rhine to Afghanistan*. Cambridge University Press. 2011.

Martinage, Robert. *Toward a new Offset Strategy.* Center for Strategic and Budgetary Assessments. 2014. http://csbaonline.org/search/?q=offset+&x=6&y=11.

http://thediplomat.com/2015/03/what-can-the-middle-ages-teach-us-about-us-naval-strategy/.

Scharre & Horowitz. *An Introduction to Autonomy in Weapon Systems*, Center for a New American Security, February 2015.

Wagner, Breanne. *Battlefield Energy*. National Defense Magazine. Abril 2007.

http://docsetools.com/articulos-enciclopedicos/article_87425.html.

Adamsky, Dmitry (Dima) *Disuasión y Ciberespacio*. La Vanguardia Dosier nº 54. 11 diciembre 2014.

Misirolli, Antonio, Stang Gerald y otros. *A changing global environment.* European Union. Institute for Security Studies. Chaillot Papers nº 133. December 2014.

Deni, John R. *New Realities. Energy Security in the 2010s and implications for US military.* US Army War College. February 2015.

http://dx.doi.org/10.1080/04597222.2015.996336.

http://govcomm.harris.com/solutions/products/defense/hamr.asp.

CAPÍTULO 3

ASPECTOS LEGALES Y ÉTICOS DE LAS TECNOLOGÍAS DISRUPTIVAS

Resumen

Albert Einstein dijo: *"No sé cómo será la tercera guerra mundial, sólo sé que la cuarta será con piedras y lanzas"*.

Pero si Albert Einstein viviera, quizás cambiaría la frase por esta otra: la cuarta guerra mundial será con humanos y máquinas.

Aunque la Humanidad se ha visto envuelta en guerras a lo largo de años y años, seguramente en ningún tiempo pasado el combatiente se ha encontrado en una situación tan compleja desde el punto de vista ético y legal como en fecha actual.

En este capítulo, analizaremos el modo el que los Estados preparan sus leyes para la Defensa y adquisición de capacidades, pero también mostraremos las limitaciones legales y la brecha que existe para regular el uso de armas autónomas, robots y sistemas no tripulados (drones y vehículos).

Palabras clave

Tecnología disruptiva, Defensa, Moral, Ética, Moral, Ciberdefensa, Ciberseguridad, Ciberguerra, Propiedad intelectual, armas autónomas

Abstract

Albert Einstein said: "I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones".

However, if Albert Einstein were alive today, perhaps he would change the sentence by the following: World War IV will be with humans and machines.

Although humanity has been embroiled in wars over years and years, surely on any time spent the combatant have been found in such a complex situation in terms of ethical and lawful as at present.

In this chapter we will discuss the way the States prepare their laws for their defines and for acquiring skills, but also we will show you the legal limitations and the existing gap to regulate the use of autonomous weapons, robots and unmanned systems (drones and vehicles).

Keywords

Disruptive technology, Defense, Cyber War, Humanitarian Law, Information, Personal data, Moral, Ethical, Autonomous weapon.

INTRODUCCIÓN

La revolución digital ha causado profundos cambios provocados por la convergencia de la informática, las comunicaciones y las tecnologías, convirtiendo a estas por un lado, en herramientas necesarias para el desarrollo de las naciones y de su seguridad y por otro lado, en elementos de riesgo de los derechos de las personas, de la seguridad nacional y de las economías de mercado.

La humanidad ha cambiado y las tecnologías de la información y la comunicación han supuesto una ruptura decisiva con las prácticas anteriores en muchos ámbitos como el social, sanitario, comercial, educativo, energético, consumo, administración, la seguridad, defensa u otros. En definitiva, tanto los sectores esenciales como otros sectores se han visto afectados por las tecnologías y según los expertos, aunque en la actualidad ya convivimos con la tecnología en casi todos los ámbitos de nuestra vida, ésta aún causará un impacto mayor en la Humanidad.

La pregunta que cabría hacerse es sí los modelos éticos y legales continúan siendo patrones o reglas válidas para la humanidad o nos enfrentamos a nuevos retos que nos llevan a otra incógnita, sí estamos preparados para afrontar dichos retos.

La opinión mayoritaria es que nos encontramos con un marco tecnológico de "innovación disruptiva" que ha abierto una brecha en los tres campos mencionados, el ético, el moral y el legal. Se trata, según los sociólogos y pensadores, de una revolución que no tiene precedentes.

Internet, como plataforma mundial, se ha convertido en parte integrante de la sociedad actual y en un bien público, cuyo buen funcionamiento es de interés general para todo el planeta. Por ello, el llamado ciberespacio ha de ser protegido de incidentes, actividades malintencionadas y utilizaciones abusivas que se producen e incrementan a una velocidad alarmante.

Si los Estados no se han puesto de acuerdo en cuestiones aparentemente tan sencillas como la naturaleza jurídica del derecho de acceso y uso de internet,[56] pocas dudas nos quedan sobre las dificultades que para aquéllos entraña la regulación de otros aspectos como el uso de la tecnología en el ámbito de la Defensa, y más en particular, el uso de armas "cibernéticas", teniendo en cuenta la necesaria reflexión previa de orden moral y ética que todo ello conlleva sobre, "hacía dónde debería caminar la Humanidad".

56 El Comité de las Regiones (órgano consultivo que representa a los entes regionales y locales de la Unión Europea) recomienda declarar el uso de internet como un derecho cívico inalienable, a cuya aplicación pueden contribuir las autoridades nacionales, locales y regionales en el marco de sus competencias, frente a las voces que lo reconocen como un derecho humano o una mera tecnología que permite ejercer los derechos fundamentales.

Si el ordenamiento jurídico internacional regulado por el llamado Derecho Internacional[57] ya se presentaba como una disciplina jurídica especialmente problemática y compleja, con la llegada de internet y las tecnologías, se han abierto aún más lagunas e insuficiencias.

Parece haber unanimidad en el hecho de que los Estados deben ponerse de acuerdo para generar y crear las normas del Derecho Internacional que regulen la convivencia de los Estados en el Ciberespacio y el uso de las armas cibernéticas por la Humanidad.[58] En esta encomienda también será preciso analizar si las llamadas "normas de la guerra" o normas de conducción de hostilidades que teníamos hasta la fecha, son útiles en un momento donde los "campos de enfrentamiento" no sólo son aquellos separados por fronteras sino también, los del Ciberespacio, donde las fronteras físicas o territoriales han desaparecido.[59]

El régimen legal aplicable a los conflictos entre Estados establecido por el Derecho Internacional no impone a éstos la obligación de llegar a una solución, sino que únicamente pesa sobre ellos la obligación de procurar *"de buena fe y con espíritu de cooperación"* una solución de la controversia.[60]

Como indica José Antonio Pastor Ridruejo,[61] *cuando la situación de conflicto entre dos o más Estados llega a una circunstancia extrema de empleo de fuerza armada, los países*

57 Disciplina reguladora de los conflictos con un componente de extranjería o internacional, bien entre Estados (Derecho Internacional Público) bien entre particulares (Derecho Internacional Privado).

58 En el documento "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: La política y la gobernanza de internet - El papel de Europa en la configuración de la gobernanza de internet", el Comité de las Regiones ya pone de manifiesto que la gobernanza de internet es una cuestión multilateral.

59 No obstante, también podríamos poner en tela de juicio si realmente existen o no las fronteras en el ciberespacio. El 28 de febrero de 2013, la Comisión Europea presentó sendas propuestas para crear un Sistema de Entrada/Salida y un Programa de Registro de Viajeros para el espacio Schengen, denominado en su conjunto «Fronteras inteligentes» junto con una propuesta de modificación del Código de fronteras Schengen. La propuesta del EES se refiere a un sistema inicialmente basado en los datos personales necesarios para identificar personas (en el texto denominados simplemente «datos alfanuméricos»), tras lo cual, al cabo de tres años, se introducirán los «datos biométricos». Transcurridos dos años, deberá evaluarse si debe permitirse el acceso a las autoridades policiales y terceros países.

60 Carta de las Naciones Unidas, artículo 33. 1) Las partes en una controversia cuya continuación sea susceptible de poner en peligro el mantenimiento de la paz y la seguridad internacionales tratarán de buscarle solución, ante todo, mediante la negociación, la investigación, la mediación, la conciliación, el arbitraje, el arreglo judicial, el recurso a organismos o acuerdos regionales u otros medios pacíficos de su elección.

61 José Antonio Pastor Ridruejo. Curso Internacional de Derecho Internacional Público y Organizaciones Internacionales. Editorial Tecnos. Grupo Anaya S.A., 2008.

entran en guerra ante lo cual el Derecho Internacional ha sentado los siguientes criterios que, seguramente, hoy podrían ser cuestionados o al menos, deberían ser revisados:

- *Condiciones en que es lícito el recurso a la fuerza armada o ius ad bellum.*
- *Eliminación de los medios de hacer guerra, esto es, el desarme.*
- *Límites a la violencia bélica mediante la regulación del comportamiento de los beligerantes durante las hostilidades, es decir, ius in bello.*
- *Posición de los terceros Estados, esto es, neutralidad.*

El artículo 2 de la Carta de Naciones Unidas, en su apartado cuarto, establece la obligación de los Miembros de la Organización en sus relaciones internacionales, *de abstenerse a recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas.*

Sin entrar en mayores valoraciones y admitiendo las discusiones interpretativas habidas en relación con el "tipo de fuerza" a que hace alusión esta disposición (véase que no menciona exactamente el término "armada") o el alcance de la "integridad territorial o la independencia política", hemos de concluir que en la llamada "ciberguerra" parece que estos conceptos podrían quedar diluidos.

Esta misma cuestión se ha planteado Timothy Edgar[62] al cuestionar, *sí cuando hablamos de ciberguerras las armas cibernéticas modifican las leyes de la guerra y en todo caso, sí los ataques cibernéticos cumplen las condiciones de un ataque armado según el Derecho Internacional, teniendo en cuenta que no resultan heridos, no hay muertes y no hay propiedades físicas destruidas.*

En todo caso, de acuerdo con el artículo 51 de la Carta de Naciones Unidas, el derecho al uso de la fuerza tendría una excepción: la legítima defensa. Así, según establece, *"ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas (...)*.

Pero qué debemos entender hoy en día como un "ataque armado". Nos asaltan dudas sobre sí en algún caso un "ciberataque" (un ataque en internet) podría suponer un "ataque armado", o sí este ataque es exclusivo del mundo "*offline*", incluso aunque las armas utilizadas sean autónomas como un dron (avión no tripulado) o un robot. En definitiva, ¿puede la soberanía de un Estado también ser violada por ataques desde el ciberespacio?

62 *La Vanguardia Ediciones. Revista Vanguardia Dossier nº 54, (Ejemplar dedicado a: La ciberguerra) Timothy Edgar. ¿Modifican las armas cibernéticas las leyes sobre la guerra?*, págs. 26-31. http://www.lavanguardia.com/internacional/20141211/54421704765/la-ciberguerra-vanguardia-dossier.html.

La "Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección" obligó a los Estados miembros de la Unión Europea al desarrollo de normas internas[63] para optimizar la seguridad de las infraestructuras críticas contra agresiones deliberadas y, muy especialmente, contra ataques terroristas. Pero la Directiva precisó que la norma de protección debería regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo, tanto de carácter físico como cibernético.

El Legislador europeo consideró prioridades estratégicas de la Seguridad Nacional a las infraestructuras *estratégicas* sitas en cualquier Estado miembro de la Unión Europea cuyo funcionamiento es indispensable y no permite soluciones alternativas y en consecuencia, hizo elaborar una norma cuyo objeto fue, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. ¿Qué ocurriría si uno de estos ataques deliberados contra una infraestructura crítica del Estado fuera llevado a cabo a través de la red bajo instrucciones o dirección del Gobierno de otro Estado?.

Jesús Reguera Sánchez[64] ha analizado también algunos aspectos de los "ciberconflictos" y de la posibilidad que existe de que éstos conduzcan a una guerra y ha concluido que, *desde una breve interpretación de la aplicación del Derecho Internacional Humanitario a la ciberguerra, se ha podido constatar que existen importantes problemas pendientes: La dificultad de identificar actores y responsabilidades, el uso de la fuerza y la legítima defensa basada en los efectos, el problema de saber diferenciar bienes de interés civil y militar ante la interconexión de la red, la participación directa en las hostilidades en la ciberguerra, entre otras; no hacen más que corroborar la sensación de falta de legislación.*

En todo caso y retomando el hilo del Derecho Internacional, traemos otro tema a discusión: el de los derechos de priosioneros y víctimas. En este punto s preciso recordar que los llamados "Derecho de la Haya y Derecho de Ginebra" vinieron a establecer una serie de normas en el marco del "derecho de la guerra" para la protección de las víctimas y la conducción de las hostilidades.

63 Fruto de dicha Directiva es la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras Críticas, que además crea el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), órgano que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas.

64 "Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario" publicado por Jesús Reguera Sánchez el 18/03/2015 y disponible en http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

Así, tras la primera y segunda guerra mundial muchos Estados participaron en negociaciones y consultas destinadas a la aprobación de tratados que regulaban entre otras cuestiones, la protección de los prisioneros de guerra y víctimas, la prohibición de empleo de gases asfixiantes tóxicos o similares o la prohibición de medios bacteriológicos en el combate. En definitiva, con el escenario fáctico resultante de las citadas guerras, se analizaron los problemas jurídicos destinados básicamente a la protección de la población civil, la protección de víctimas de guerra y la regulación de las normas de combate, todo ello siempre con el fin último de proteger los derechos de las personas.

Nació así el llamado "Derecho Internacional Humanitario" como una rama del Derecho Internacional destinado a limitar y evitar el sufrimiento humano en tiempo de conflicto armado con el objetivo de proteger a personas civiles y personas que ya no estén participando en hostilidades.

Distinto del Derecho Internacional Humanitario (aunque podría decirse que no cabe hablar de uno sin mencionar el otro) es el Derecho de los Derechos Humanos, cuyo fin es el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana. La Declaración Universal de Derechos Humanos recoge las características básicas de estos principios como su universalidad, interdependencia, indivisibilidad, igualdad y no discriminación.

Durante décadas este marco legal ha servido a los intereses perseguidos por las Naciones para garantizar no sólo los derechos de los individuos en tiempos de paz, sino también los derechos de las víctimas en tiempos de guerra y las normas de enfrentamiento.

Pero también en este escenario, la revolución digital ha introducido dudas, lagunas y reflexiones que reconducen a un nuevo punto de inicio, haciendo tambalear la estructura jurídica internacional.

Quizás no sea tanto un problema de principios y valores sino de cómo volver a instrumentarlos. ¿Debemos tomar nuevas medidas en el marco de los Derechos Humanos y el Derecho Internacional Humanitario frente al abuso de las tecnologías y plataformas digitales como medios de difusión de las condiciones en que son capturados tratados y abatidos rehenes de grupos terroristas y víctimas de enfrentamientos bélicos con la consiguiente vulneración de su derecho al honor e intimidad personal o la de sus familiares?

O por el contrario debemos entender como parte del progreso y del Derecho a la Información, que la comunidad internacional hoy en día tenga acceso "en vivo y en directo" a los horrores de las guerras, situaciones de conflicto y a los actos de terrorismo.[65]

65 A través de internet asistimos a actos terroristas como degollamientos o matanzas de rehenes, bombardeos selectivos en situaciones de conflicto y otros hechos similares como "espectadores de

Aunque por el momento parece que hay consenso en que las leyes y normas aplicables en otros ámbitos de nuestras vidas cotidianas lo son también en el Ciberespacio, posiblemente la dimensión de los daños morales derivados de las situaciones mencionadas en el apartado anterior que pueden causar las tecnologías (en particular en relación con los derechos fundamentales a la libertad de expresión, intimidad y protección de datos), no estaba contemplada en las normas y leyes elaboradas hace décadas.

Jesús Reguera Sánchez[66] indica sobre este asunto que, *tras los incidentes causados en abril de 2007 por el traslado en la ciudad de Tallin del monumento a los soldados soviéticos caídos durante la Segunda Guerra Mundial (desde el centro de la ciudad hasta el cementerio militar) se produjeron unos ciberataques contra los sistemas de información del gobierno estonio, por agresores no identificados cuyo resultado fue la paralización de gran parte de la administración de Estonia.*

La consecuencia más inmediata fue que la OTAN decidió establecer en su capital, Tallin, el Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN y una de las primeras iniciativas de este Centro, fue la convocatoria de un Grupo Internacional de Expertos (GIE) en defensa, ciberseguridad y Derecho internacional, para que trabajaran en lo que pudiera ser el equivalente de la Convención de Ginebra sobre el Derecho Internacional Humanitario, aplicado a los conflictos en el ciberespacio.

El resultado fue el Manual de Tallin, dirigido por el Profesor Michael Schmitt de la U.S. Naval War College. La premisa fundamental para redactar este Manual fue que "la guerra no deja de ser tal porque se lleve a cabo en el ciberespacio", es decir, es posible la guerra en el ciberespacio.

Aunque la Unión Europea no defiende la creación de nuevos instrumentos jurídicos internacionales para abordar las cuestiones relacionadas con el Ciberespacio,[67] no

primera fila sobre el terreno de combate".

66 "Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario" publicado por Jesús Reguera Sánchez el 18/03/2015 y disponible en http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

67 En esta línea encontramos diversos documentos, véase por ej. el documento de 22 de julio de 2013 sobre las Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro" cuando indica en su apartado 6 reconoce que, *el Derecho internacional, incluidos convenios internacionales como el Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) y los correspondientes convenios en materia de Derecho humanitario y derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos, el Pacto internacional relativo a los derechos económicos, sociales y culturales, proporcionan un marco jurídico aplicable al ciberespacio. Por todo ello, deberá procurarse que dichos instrumentos sean también de aplicación en el ciberespacio; en consecuencia, la UE no defiende la creación de nuevos*

obstante, indica que es preciso examinar de qué modo puede garantizarse que esas disposiciones se apliquen también en el Ciberespacio, haciendo especial hincapié en que deberán respetarse "*en línea*" las obligaciones jurídicas establecidas en el Pacto Internacional de Derechos Civiles y Políticos, el Convenio Europeo de Derechos Humanos y la Carta de los Derechos Fundamentales de la Unión Europea.

Una conclusión parece evidente, todas las reglas han cambiado.

EL CIBERESPACIO: UN NUEVO CAMPO DE BATALLA PARA LA CIBERDELINCUENCIA, CIBERTERRORISMO Y CIBERGUERRAS

Introducción

En enero de 2001, la Comisión Europea dirigió al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones una comunicación sobre la creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.[68]

En dicha comunicación, la propia Unión Europea reconoce que la Internet sin fronteras y con múltiples niveles, se ha convertido en uno de los instrumentos más poderosos del progreso mundial pero también con mayores riesgos, sin tutela ni la reglamentación de los Estados, pese a que, como ya hemos visto anteriormente, para los Estados, las leyes y normas aplicables en otros ámbitos de nuestras vidas cotidianas son también aplicables en el ciberespacio.

Años más tarde, en la Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la "Estrategia de Ciberseguridad de la Unión Europea:

Un ciberespacio abierto, protegido y seguro",[69] la Unión Europea se reafirma en el actual modelo de gobernanza multilateral de Internet (el mundo digital no está controlado por una sola entidad) y pone de manifiesto que garantizar la seguridad de la red se ha convertido en una "responsabilidad compartida" donde todas las partes

instrumentos jurídicos internacionales para abordar las cuestiones relacionadas con el ciberespacio.

68 COM (2001) 298 final.

69 JOIN (2013) 1 final.

interesadas, ya sean las administraciones públicas, el sector privado o los ciudadanos, han de reconocer esta responsabilidad compartida, tomar medidas para protegerse y, en caso necesario, ofrecer una respuesta coordinada para reforzar la Ciberseguridad.[70]

No cabe duda de que el mundo digital ha aportado grandes beneficios, pero también grandes vulnerabilidades. Los incidentes de Ciberseguridad, tanto deliberados como accidentales, se incrementan a ritmo alarmante, llegando a perturbar no sólo el suministro de servicios esenciales que damos por descontados como el agua, la asistencia sanitaria, la electricidad o los servicios móviles, sino también la Seguridad Nacional de los Estados.

Las amenazas pueden tener varios orígenes, entre ellos los ataques delictivos, por motivos políticos, terroristas o incluso patrocinados por los Estados, así como catástrofes naturales o errores no intencionados.

Como se indica en el documento "Guerra cibernética: Aspectos Organizativos" del Grupo de Trabajo nº 3 del CESEDEN,[71] *los ciberataques han pasado a invadir todos los sectores de la actividad individual y colectiva de nuestra sociedad, haciéndose más fácil atacar una red que defenderla, por la enorme desproporción entre el esfuerzo necesario para un ataque cibernético, amparado en el anonimato, con la ventaja para el atacante de elegir el momento y el objetivo, y el necesario para la protección de los sistemas.*

Ello ha conducido al enfrentamiento de amenazas y hechos reales constitutivos de actos ilícitos civil y penalmente, actos terroristas y en definitiva actos que ponen en peligro nuestros sistemas físicos incluyendo nuestros sistemas militares. Por ello, la ciberdefensa ha pasado a ser un nuevo dominio de guerra, prueba de lo cual, más de 140 países, entre ellos España, están ya desarrollando sus capacidades.

Así lo manifiesta igualmente el Grupo de Trabajo Nº 3 del CESEDEN que asegura, *"se ha dicho del Ciberespacio que es el campo de batalla del futuro".*[72]

70 En la misma línea, la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: La política y la gobernanza de internet - El papel de Europa en la configuración de la gobernanza de internet.

71 XXXIII Curso de Defensa Nacional, Ciberseguridad nuevo reto del siglo XXI: Aspectos Organizativos. Grupo de Trabajo nº 3 del CESEDEN.

72 XXXIII Curso de Defensa Nacional, Ciberseguridad nuevo reto del siglo XXI: Aspectos Organizativos. Grupo de Trabajo nº 3 del CESEDEN: El problema fundamental para la Defensa es el cambio que las nuevas tecnologías han producido. Si en el pasado era suficiente con aprovecharse de las nuevas capacidades de los sistemas de información y del ciberespacio para mejorar la eficacia operacional de las Fuerzas Armadas, ahora es necesario poder combatir, y ganar, en el ciberespacio. La Defensa requiere asegurar las capacidades en el ciberespacio para poder garantizar la efectividad en las operaciones tradicionales. Este cambio obliga a modificar los conceptos y doctrinas que se aplican a la confrontación clásica, que deben ser adaptados a las exigencias de un escenario virtual.

El convenio sobre Ciberdelincuencia del Consejo de Europa, firmado en Budapest el 23 de noviembre de 2001 (y ratificado por España en el año 2010) ya puso de manifiesto que los ataques informáticos eran casi un "negocio al alza".

El problema en el que nos encontramos con la irrupción de la tecnología como un nuevo instrumento de ataque, tal como hemos visto en el punto anterior, es llevar a cabo la separación jurídica entre un acto criminal en la red, un acto de ciberterrorismo (normalmente son actos con fines políticos o religiosos) y un acto de ciberguerra.

Aparentemente podría resultar sencillo, pero en la práctica no lo es.

Por otro lado, desde el final de la Guerra Fría, tanto en Europa como en Estados Unidos se han revisado las estrategias de defensa, llevándose a cabo acciones como la remodelación de las fuerzas armadas o la reducción del gasto en el sector.

En la actualidad estas estrategias tienen en cuenta la búsqueda de la "ciberseguridad" no sólo a causa del aumento de los riesgos y amenazas que pueden poner en riesgo los servicios prestados por las Administraciones Públicas, las Infraestructuras Críticas o las actividades de las empresas y ciudadanos, sino también ante la evidencia de que, determinados países disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional. Por ello, criterios como el de la reducción del gasto en el sector deberían ser revisados de nuevo, de cara a valorar las necesidades de inversión no sólo en tecnología sino también en innovación que la Seguridad y Defensa requieren actualmente.

Los Estados son conscientes de que ahora, la política de Seguridad y Defensa son cuestiones fundamentales junto con la base tecnológica e industrial que son, estas últimas, las que generan las capacidades necesarias para afrontar los retos de la Defensa y también los de la seguridad.

En esta línea, el ex Secretario de Defensa de los Estados Unidos Chuck Hagel, en su discurso de 3 de septiembre de 2014, advirtió de que las tecnologías disruptivas y las armas destructivas que antes sólo estaban en manos de los estados más avanzados han proliferado y están siendo adquiridas por países en desarrollo y grupos terroristas.[73]

En noviembre de 2014 el Departamento de Defensa de EEUU adoptó la tercera estrategia de compensación, "O*ffset Strategy", para preservar su capacidad de proyección militar y compensar las dificultades a las que se enfrentaba la actual,*[74] *consciente de que*

73 U.S. Department of Defense, "Defense Innovation Days" by Secretary of Defense Chuck Hagel, Newport, Rhode Island, Wednesday, September 03, 2014. http://www.defense.gov/speeches/speech.aspx?speechid=1877

74 Real Instituto Elcano, 2015 Artículo Offset Strategy: ¿hacia un nuevo paradigma de defensa en EEUU? Autor Luis Simón. http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/Elcano_es/Zonas_es/ARI14-2015-Simon-offset-strategy-hacia-un-nuevo-paradigma-de-defensa-en-EEUU

el dominio estadounidense en los mares, en los cielos, en el espacio y en el ciberespacio ya no se puede dar por sentado, pudiendo tener que enfrentarse a un arsenal de tecnologías avanzadas y disruptivas que impiden sus ventajas tecnológicas y limitan su libertad de maniobra.

En su discurso Chuck Hagel también puso de manifiesto que el siglo XXI ofrece nuevos desafíos y que en la actualidad no es posible asumir -como se hizo en la década de 1950 y 70- *"que el Departamento de Defensa será la única fuente de las tecnologías clave de vanguardia"*.

Según el ex Secretario de Defensa *"hoy en día, muchos de los cambios tecnológicos sin precedentes -en áreas como la robótica, la informática avanzada, la miniaturización y la impresión en 3D- proviene del sector comercial. El Departamento de Defensa debe ser capaz de evaluar qué innovaciones comerciales tienen potencial militar, rápidamente adoptarlas y probarlos, incluso a través de "juegos de guerra" y demostraciones"*.

En todo caso ha quedado claro que la Ciberseguridad se ha convertido en una necesidad no sólo para el mundo civil sino también para la estabilidad de la paz entre los países con la peculiaridad de que, en internet no existen fronteras, éstas se difuminan y con ellas también las fronteras entre la seguridad interior y exterior, siendo necesario por tanto mejorar la coordinación de políticas y normas de derecho entre los Estados.

La Unión Europa ha aclarado los principios que deben presidir la política de ciberseguridad tanto en la propia Unión Europea como a escala internacional así como las prioridades y medidas estratégicas, en la "Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Estrategia de Ciberseguridad de la Unión Europea: un Ciberespacio abierto, protegido y seguro"[75].

Principios que deben presidir el Ciberespacio

En relación con los principios que deben presidir el Ciberespacio, la Unión Europea aboga por los siguientes:

a) Las leyes y normas aplicables en otros ámbitos de nuestras vidas cotidianas lo son también en el ciberespacio.

b) La Ciberseguridad solo puede resultar positiva y eficaz si se basa en los derechos fundamentales y las libertades enunciados en la Carta de los Derechos

75 Nº de Doc.: JOIN (2013) 1 final.

Fundamentales de la Unión Europea y en los valores esenciales. Los derechos individuales no pueden protegerse sin redes y sistemas seguros.

c) Todos los ciudadanos deberían poder acceder a Internet y a un flujo de información libre de trabas. Deben garantizarse la integridad y la seguridad de Internet para así hacer posible un acceso seguro para todos.

d) El mundo digital no está controlado por una sola entidad. Actualmente intervienen en él varias partes, muchas de las cuales son entidades comerciales y no gubernamentales que participan en la gestión diaria de los recursos, protocolos y normas de Internet y en su futuro desarrollo. La Unión Europea reafirma la importancia de todas las partes interesadas en el actual modelo de gobernanza de Internet y respalda este planteamiento de gobernanza multilateral.

e) Todas las partes interesadas, ya sean las administraciones públicas, el sector privado o los ciudadanos, han de reconocer una responsabilidad compartida en la seguridad de las redes y la información, en la toma de medidas para protegerse y, en caso necesario, ofrecer una respuesta coordinada para reforzar la ciberseguridad.

Medidas Estratégicas de la Unión Europea en relación con el Ciberespacio

Las prioridades y medidas estratégicas que la Unión Europea plantea para resolver los problemas de seguridad de internet o la ciberseguridad se articulan en torno a las siguientes:

a) Lograr la ciberresiliencia para lo cual, tanto las administraciones públicas como el sector privado deben desarrollar capacidades y cooperar efectivamente. Para ello, en Europa se han adoptado diversos tipos de medidas.

Por un lado, a través de diversas Directivas, se ha obligado a proveedores de comunicaciones electrónicas a gestionar adecuadamente los riesgos a que se enfrentan sus redes y a notificar las violaciones significativas de la seguridad.

También la normativa de la Unión Europea sobre protección de datos establece que los responsables del tratamiento han de prever requisitos y salvaguardias que garanticen la protección de los datos personales, entre ellos las medidas de seguridad.

Por otro lado, en el año 2004 se creó la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y en el año 2012 se creó con carácter permanente un equipo de respuesta a emergencias informáticas, responsable de la seguridad

de los sistemas de Tecnologías de la Información de las instituciones, agencias y organismos de la Unión Europea (CERT[76]-UE).

Pero pese a ello, se observan lagunas especialmente en lo tocante al compromiso del sector privado, a las capacidades nacionales y a la coordinación ante incidentes que traspasan las fronteras.

b) Reducir drásticamente la ciberdelincuencia y dado que ésta no conoce fronteras, los cuerpos de seguridad deberían adoptar un enfoque transfronterizo coordinado y colaborativo para responder esta amenaza creciente. En este punto, la Unión Europea es consciente de que los Estados miembros necesitan una normativa rigurosa y eficaz para luchar contra la ciberdelincuencia. El Convenio sobre la Ciberdelincuencia del Consejo de Europa, también denominado Convenio de Budapest, es un tratado internacional vinculante que ofrece un marco efectivo para la adopción de normas nacionales. Junto a dicho Convenio, también se han adoptado actos legislativos sobre la ciberdelincuencia, entre ellos varias directivas.

c) Desarrollar estrategias y capacidades de Ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD). En definitiva, los esfuerzos de Ciberseguridad de la Unión Europea entrañan asimismo una dimensión de Ciberdefensa. Según la Unión Europea, ante tan polifacéticas amenazas, conviene potenciar las sinergias entre los enfoques civil y militar para la protección de ciberactivos críticos. De hecho, para evitar duplicidades, la Unión Europea examina de qué modo pueden ella y la OTAN aunar sus esfuerzos para aumentar la resiliencia de infraestructuras críticas públicas, de Defensa y de información de las que dependen los miembros de ambas organizaciones.

d) Desarrollar recursos industriales y tecnológicos de Ciberseguridad. Aunque Europa dispone de excelentes capacidades de investigación y desarrollo, muchas de las empresas punteras mundiales proveedoras de productos y servicios de tecnologías de la información y la comunicación innovadores, están establecidas fuera de la Unión Europea.

Se alcanzaría un nivel elevado de seguridad si todos los que intervienen en la cadena de valor (fabricantes de equipos, desarrolladores de programas informáticos, proveedores de servicios de la sociedad de la información, etc.) hacen de la seguridad un objetivo prioritario. La Comisión respalda la elaboración de normas de seguridad y presta asistencia en los regímenes de certificación voluntarios en el campo de la computación en nube.

Esta certificación se inspira en las actividades de normalización en curso de las organizaciones europeas de normalización (CEN, CENELEC y ETSI),

76 Por sus siglas en inglés "*Computer Emergency Response Team*"..

del Grupo de Coordinación de Ciberseguridad (CSCG), así como en los conocimientos y experiencia de la ENISA, la Comisión y otras partes interesadas.

e) Establecer una política internacional coherente del Ciberespacio para la Unión Europea y promover los valores esenciales de la Unión Europea. Esto es un reto mundial al que la Unión Europea se debe enfrentar junto con los socios y organizaciones internacionales pertinentes.

La cooperación como medida de seguridad en el Ciberespacio

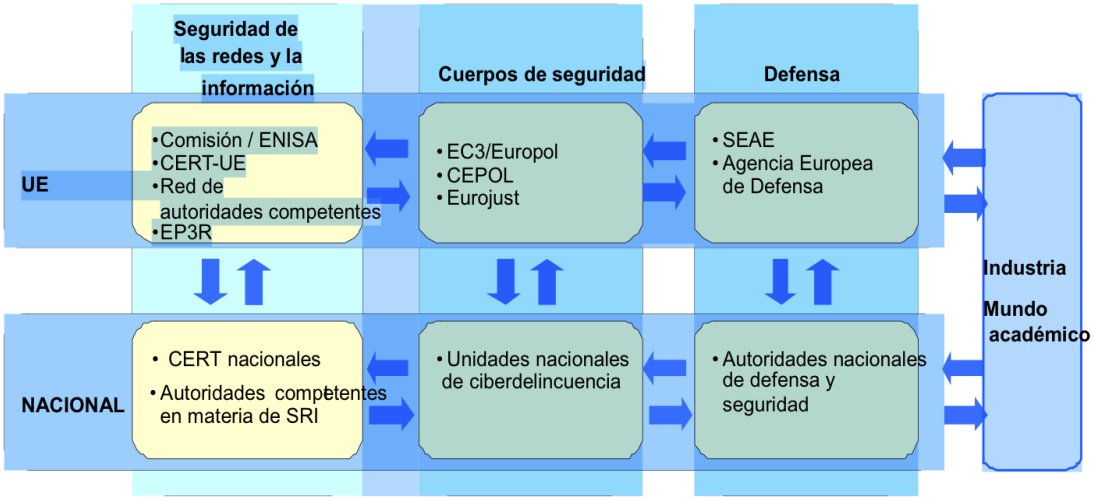
En la misma "Comunicación de la Unión Europea sobre un Ciberespacio abierto, protegido y seguro" se aboga por la coordinación entre autoridades competentes en materia de seguridad de redes e información, cuerpos de Seguridad y Defensa.

En esta línea, para hacer frente a los problemas mundiales que plantea el Ciberespacio, la Unión Europea procura cooperar estrechamente con organizaciones que trabajan en este campo, como el Consejo de Europa, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), las Naciones Unidas, la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Organización del Tratado del Atlántico Norte (OTAN), la Unión Africana (UA), la Asociación de Naciones del Sudeste Asiático (ASEAN) y la Organización de los Estados Americanos (OEA).

A nivel bilateral, la cooperación con los Estados Unidos reviste especial importancia en materia de Ciberseguridad y Ciberdelincuencia.

A a escala nacional, se indica que (i) los Estados miembros deberían disponer, ya en la actualidad, de estructuras para abordar la Ciberresiliencia, la Ciberdelincuencia y la Ciberdefensa y (ii) deberán establecer en sus estrategias nacionales de Ciberseguridad las funciones y responsabilidades de sus diversas entidades nacionales.

A escala de la Unión Europea (como ocurre a escala nacional) se señala que hay distintas entidades responsables de la ciberseguridad como son la Agencia Europea de Seguridad de las Redes y la Información (ENISA), el Centro Europeo contra el Cibercrimen (Europol/EC3) y la Agencia Europea de Defensa (AED), los cuerpos de seguridad y la Defensa, los cuales han de colaborar, manteniendo al mismo tiempo sus especificidades.



(Cuadro esquemático de los Órganos de los Estados Miembros y la Unión Europea en materia de seguridad y Defensa. Imagen extraída 1 cuadro extraído de la Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro Bruselas, 7.2.2013 JOIN(2013) 1 final)[77]

A escala internacional la Comisión Europea y el Alto Representante[78] garantizan, junto con los Estados miembros, una actuación internacional coordinada en el ámbito de la Ciberseguridad.

En este marco, la Comisión, el Alto Representante y los Estados miembros mantienen diálogos políticos con los socios internacionales y organizaciones internacionales tales como el Consejo de Europa, la OCDE, la OSCE, la OTAN, la Asamblea General de las Naciones Unidas (AGNU), la Unión Internacional de Telecomunicaciones (UIT), la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y el Foro para la Gobernanza de Internet (IGF).

Además con motivo de la Cumbre Unión Europea - EE.UU. de 2010, se creó el Grupo de Trabajo Unión Europea -EE.UU. sobre Ciberseguridad y Ciberdelincuencia.

77 http://www.europarl.europa.eu/meetdocs/2014_2019/documents/join/com_join(2013)0001_/com_join(2013)0001_es.pdf

78 El Tratado de Lisboa creó el cargo de Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, cuyo papel consiste en dirigir la política exterior de la Unión Europea (UE).

Mecanismos de respuesta de la Unión Europea frente a los ataques en el Ciberespacio

En cuanto al apoyo ante incidentes y ataques cibernéticos graves, los mecanismos de respuesta que plantea la Unión Europea difieren en función de la naturaleza, la magnitud y los efectos transfronterizos del incidente.

- Si el incidente tiene efectos graves en la continuidad de las actividades, se propone la activación de planes de cooperación nacionales o de la Unión Europea en materia de seguridad de redes e información, según la naturaleza transfronteriza del incidente. En este contexto, se recurrirá a la red de autoridades competentes en materia de redes e información para compartir información y prestar apoyo, lo cual permitirá mantener o restaurar las redes y los servicios afectados.
- Si el incidente parece tener origen delictivo, se deberá informar a Europol/EC3 para que, junto con las autoridades policiales de los países afectados, pueda iniciar una investigación, conservar las pruebas, identificar a los autores y velar por que se castigue su delito.
- Si el incidente parece estar relacionado con el ciberespionaje o con un ataque promovido por un Estado, o afecta a la Seguridad Nacional, las autoridades policiales y de Defensa Nacionales deberán alertar a sus homólogos de que sufren un ataque y se hallan en condiciones de defenderse. Entonces se activarán mecanismos de alerta temprana y, en caso necesario, procedimientos de gestión de crisis o de otros tipos. Un incidente o ataque cibernético de especial gravedad podría ser motivo suficiente para que un Estado miembro invocara la cláusula de solidaridad de la Unión Europea (artículo 222 del Tratado de Funcionamiento de la Unión Europea).
- Si el incidente parece haber comprometido datos personales, intervendrán las autoridades nacionales responsables de la protección de datos o la autoridad reguladora nacional, de conformidad con la Directiva 2002/58/CE.
- Por último, la gestión de ciberincidentes y ciberataques se verá facilitada por el apoyo de las redes de contacto y el apoyo de los socios internacionales, con medidas técnicas de atenuación, investigaciones penales o la activación de mecanismos de gestión de crisis y respuesta.

Medidas a futuro propuestas por la Unión Europea para la seguridad de las redes e información del Ciberespacio

Actualmente la Unión Europea se encuentra en plena elaboración de una nueva directiva para garantizar un elevado nivel común de seguridad de las redes y de la información[79] para lo cual:

a) Establece las obligaciones que han de cumplir todos los Estados miembros en materia de prevención, gestión y respuesta a riesgos e incidentes que afecten a las redes y los sistemas de información;

b) Establece un mecanismo de cooperación entre los Estados miembros con el fin de garantizar la aplicación uniforme de la Directiva en la Unión y, en su caso, una gestión y una respuesta eficaces y coordinadas ante los riesgos e incidentes que afecten a las redes y los sistemas de información;

c) Establece requisitos en materia de seguridad para los operadores del mercado y las administraciones públicas.

Se trata de un nuevo reto en la lucha contra la Ciberdelincuencia a través de cuyo texto Europa reglamentará, entre otras cuestiones, (i) la estrategia nacional de seguridad de las redes y la información y el plan de cooperación nacional en esta materia, (ii) la autoridad nacional competente en materia de seguridad de las redes y los sistemas de información, (iii) la obligación de crear un equipo de respuesta a emergencias informáticas (CERT), (iv) la creación de una red de cooperación para colaborar contra los riesgos e incidentes que afecten a las redes y los sistemas de información, (v) los sistema seguros de intercambio de información dentro de la red de cooperación, (vi) las alertas tempranas y su difusión, (vii) la respuesta coordinada de las autoridades, (viii) el Plan de cooperación de la Unión Europa y (ix) la cooperación internacional

En cuanto a la política de seguridad en materia de Ciberdefensa, con el fin de mantenerse al día con el cambiante panorama de amenazas y mantener una sólida Defensa cibernética, la OTAN ha adoptado una nueva política mejorada y su plan de acción, la cual fue aprobada por los Aliados en la Cumbre de Gales en septiembre de 2014. La política establece que la Ciberdefensa es parte de la tarea principal de la Alianza de defensa colectiva, confirma que el derecho internacional se aplica en el ciberespacio e intensifica la cooperación de la OTAN con la industria. La principal prioridad es la protección de los sistemas de comunicaciones de propiedad y operados por la Alianza.

79 Nº de Doc.: COM (2013) 48 final: Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión.

La Estrategia de Seguridad Española

A nivel interno en España, la Directiva de Defensa Nacional 1/2012, promulgada el 31 de julio la denominada "Por una defensa necesaria, por una defensa responsable", menciona específicamente los riesgos derivados de un mundo cada vez más interconectado, en el que grupos terroristas y de delincuencia organizada pueden dañar gravemente la paz social, la seguridad ciudadana, la estabilidad política y la prosperidad general.

Para hacer frente a los nuevos riesgos emergentes de un mundo globalizado, la Directiva subraya que la Alianza Atlántica sigue siendo el vínculo de Defensa y Seguridad colectiva más apropiado para España, y con la finalidad de alcanzar los objetivos marcados en las "líneas generales", se insta a promover una aproximación integral a la Ciberseguridad.[80]

Además, la Directiva identifica como necesidades de la Defensa, por un lado, el reforzamiento de los sistemas de obtención de información y de elaboración de inteligencia para apoyar a las operaciones, y por otro lado, el reforzamiento de los sistemas de mando y control para reducir el riesgo de ataques cibernéticos.

La "Estrategia de Ciberseguridad Nacional" aprobada por el Gobierno de España[81] e impulsada por el Consejo de Seguridad Nacional pretende dar respuesta al enorme desafío que supone la preservación del Ciberespacio, de los riesgos y amenazas que se ciernen sobre él, poniendo de manifiesto nuestras capacidades colectivas implicando a la coordinación y armonización de todos los actores y recursos del Estado, la colaboración público-privada y la participación de la ciudadanía.

Para el logro de sus objetivos, la Estrategia crea una estructura orgánica que se integra en el marco del Sistema de Seguridad Nacional. Esta estructura orgánica está constituida por los siguientes componentes bajo la dirección del Presidente del Gobierno:

- El Consejo de Seguridad Nacional;
- El Comité Especializado de Ciberseguridad;
- El Comité Especializado de Situación, único para el conjunto del Sistema de Seguridad Nacional.

80 Fuente: Ministerio de Defensa de España. http://www.defensa.gob.es/politica/seguridad-defensa/objetivos/.

81 http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf.

Estructura orgánica de la ciberseguridad nacional

(Cuadro esquema de la estructura orgánica del Centro de Seguridad Nacional. Imagen extraída del documento descriptivo de la Estrategia de ciberseguridad nacional 2013).[82]

Entre las funciones de dichos órganos, destacamos las siguientes:

- El Consejo de Seguridad Nacional se configurada como Comisión Delegada del Gobierno para la Seguridad Nacional y asiste al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.
- El Comité Especializado de Ciberseguridad da apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la Ciberseguridad. Además, refuerza las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de Ciberseguridad, así como entre los sectores públicos y privados, y facilita la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.
- El Comité Especializado de Situación es convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la Ciberseguridad que, atendiendo a la acentuada transversalidad dimensión e impacto de sus efectos, produzcan el desbordamiento de los límites de capacidad de respuesta eficaz por parte de los mecanismos habituales previstos, siempre respetando las competencias asignadas a las distintas Administraciones Públicas y a los efectos de garantizar una respuesta inmediata y eficaz a través de un solo órgano de dirección político-estratégica de la crisis.

82 http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

En otro orden de cosas, la Orden DEF/166/2015, de 21 de enero, por la que se desarrolla la organización básica de las Fuerzas Armadas, integra dentro del Estado Mayor de la Defensa el Mando Conjunto de Ciberdefensa (MCCD). El MCCD se estructura en un Estado Mayor y dos Jefaturas:

- La Jefatura de Operaciones, que será responsable de la ejecución de las operaciones de Ciberdefensa, a través de actividades de Defensa, explotación y respuesta. Así mismo, prestará el apoyo técnico necesario para el desarrollo de las citadas operaciones.
- La Jefatura de Administración y Servicios, que será responsable de prestar el apoyo administrativo, técnico y de vida y funcionamiento del MCCD.

En cuanto a sus funciones, MCCD ejerce las responsabilidades que le encomienda el artículo 15 del Real Decreto 872/2014, de 10 de octubre y en particular, entre otras, las siguientes:

a) Dirige y coordina, en materia de Ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos.

b) Ejerce la respuesta oportuna, legítima y proporcionada en el Ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

c) Define, dirige y coordina la concienciación, la formación y el adiestramiento especializado en esta materia.

d) Además, es responsable del desarrollo y detalle de las políticas de Seguridad de la Información en los Sistemas de Información y Telecomunicaciones (SEGINFOSIT) y de la dirección de la ejecución y el control del cumplimiento de estas políticas, en el ámbito del Ministerio de Defensa.

El ámbito de actuación del MCCD son las redes y los Sistemas de Información y Telecomunicaciones (CIS, por sus siglas en inglés) del Ministerio de Defensa, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional.

Visto todo lo anterior, podemos concluir que, como elemento común a la Ciberdelincuencia, Ciberterrorismo y Ciberguerras, si bien deben aplicarse *en línea* los mismos principios, valores y normas que se promueven *fuera de línea,* nos encontramos ante "asedios y ofensivas" que requieren la creación de nuevos organismos y el refuerzo de la colaboración de equipos tanto nacionales como internacionales, debiendo contemplar tanto unos como otros, expertos en materia de tecnología además de los juristas, políticos, militares y otros expertos y estrategas que tradicionalmente ya se tenían en cuenta.

LA INFORMACIÓN: UN NUEVO VALOR

Introducción

Una de las consecuencias del uso de las tecnologías es sin duda alguna la ingente cantidad de información y datos que es obtenida, almacenada y tratada por los sistemas de información y sus usuarios.

Aunque a priori pudiera parecer que la acumulación de información es una ventaja competitiva, lo cierto es que en la actualidad el procesamiento de grandes volúmenes de datos conlleva problemas de lo que se ha llamado el "big data".

El big data es el resultado del impacto que la evolución de la tecnología de tratamiento de información ha tenido sobre los procesos de generación, producción, transmisión, almacenamiento, organización, difusión y acceso a la información.

Con internet y las tecnologías en cualquier sector (civil o militar) los datos e informaciones crecen tan rápidamente que no pueden ser manipulados por las herramientas de gestión de bases de datos tradicionales.

Pero el volumen o tamaño no es el único problema al que enfrentarse para buscar soluciones: además hay que almacenar la información con las debidas medidas de seguridad, es necesario disponer de herramientas y medios para capturarla, consultarla, gestionarla y analizarla de forma rápida y eficiente.

Los sensores de los drones, vehículos no tripulados y otras tecnologías así, como la combinación de éstos en sistemas multiplataforma con aviones tripulados y otros medios, han impulsado la posibilidad de recogida de datos (todo tipo de información incluyendo audios e imágenes) en el sector de la Defensa.

Además de los problemas ya mencionados en el punto anterior (cantidad, capacidad de almacenamiento, acceso a la información, seguridad), se requiere de cuerpos expertos que conozcan las tecnologías, militares que operen las flotas, tripuladas o no, técnicos y científicos y sofisticados sistemas de big data para la explotación de los datos de forma que *se permita a las máquinas llevar a cabo su trabajo de forma eficiente*.

El resultado será un *sistema de toma de decisiones inteligentes* o un *sistema de información de apoyo* de toma de decisiones a los usuarios.

De manera que, el big data supone enfrentarnos al desafío de poder gestionar las bases de datos de información y los datos que se acumulan por el hecho de cada vez son más y diversas las fuentes de las que provienen estos.

Las herramientas tradicionales devienen obsoletas y los sistemas utilizados no permiten una gestión eficaz de la información, por el volumen, la variedad y la falta de rapidez en la disponibilidad de los datos e informaciones.

La falta de una infraestructura adecuada, la falta de conocimientos y la escasez de presupuesto para estar al día hacen que algunos expertos recomienden la externalización de los datos e informaciones en sistemas externos e incluso "en la nube".

Pero ello plantea el problema de la confidencialidad y seguridad de los datos e informaciones, fundamentalmente cuando los servicios "de la nube" se contratan de proveedor a proveedor en el Ciberespacio y el propietario de los datos pierde el control del "*tenedor*" de los mismos. Caben otras opciones como sería la de *"fabricar su propia nube"*. Pero todo ello tiene un alto coste.Además de lo anterior, cuando estas informaciones y datos se refieren a individuos o personas físicas en el ámbito de la Unión Europea, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva de protección de datos) constituye el texto de referencia, a escala europea, en materia de protección de datos personales.[83]

Esta norma crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales en el ámbito de la Unión Europea, para lo cual la norma fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos. Dicho organismo en España está constituido por la Agencia Española de Protección de Datos. Además la Directiva de protección de datos establece rígidas restricciones para llevar a cabo la transferencia internacional de datos desde entidades ubicadas en países miembros de la Unión Europea a otros terceros países.

Ahora bien, el artículo 3 de la Directiva establece que, las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea[84] y , en cualquier caso, al tratamiento de datos que tenga por objeto la Seguridad Pública, la Defensa , la Seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la segundad del Estado) y las actividades del Estado en materia penal.

83 Otros terceros países también tienen sus propias normas de protección de datos personales pero, otros tantos no.

84 Título V disposiciones generales relativas a la acción exterior de la Unión y disposiciones específicas relativas a la política exterior y de seguridad común.

Además de las anteriores exclusiones, la normativa interna en España (fruto de la transposición de la Directiva Europea de Protección de Datos), Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece en su artículo 2 que el régimen de protección de los datos de carácter personal no será de aplicación a los ficheros sometidos a la normativa sobre protección de materias clasificadas así como a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. Aunque para estos casos, nuestra norma interna establece la obligación de comunicar al órgano de control, esto es, a la Agencia Española de Protección de Datos, previamente la existencia de los ficheros.

La cuestión (y no es baladí) es dilucidar, dónde está el límite que nos señala cuándo los derechos de los individuos están protegidos por la normativa de protección de datos y cuándo no.

Otro aspecto no menos importante es el del valor de la información cuando esta información se traduce en un conjunto de algoritmos destinados a la creación de una aplicación informática, un sistema inteligente, un arma autónoma, un sistema de comportamiento de individuos o simplemente un conjunto de herramientas para securizar un entorno en el Ciberespacio.

Entramos ahora en una cuestión de propiedad intelectual y derecho de patentes y las preguntas a plantearnos serían, a quién corresponden los derechos y sí son transferibles a terceros. Se trata de derechos de propiedad sobre activos intangibles.

El marco jurídico europeo

En el año 2007 la Comisión Europea puso de manifiesto en su Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la "Estrategia para una industria europea de la Defensa más sólida y Competitiva"[85] que había claros indicios de que la industria europea de la Defensa no avanzaba debido a un marco político y jurídico inadecuado.

Fruto de dicha Comunicación y otras consideraciones, se aprobó la Directiva 2009/81/CE del Parlamento Europeo y del Consejo de 13 de julio de 2009 sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la Defensa y la Seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE.

85 Documento COM (2007) 764 final.

En el considerando 44 de dicha Directiva se indicaba expresamente que, la seguridad del abastecimiento puede implicar una gran variedad de exigencias, incluidas, por ejemplo, las normas internas de la empresa entre filial y matriz en relación con los derechos de propiedad intelectual, motivo por el cual, entre los requisitos de capacidad técnica de los operadores económicos (esto es, del contratista, proveedor o prestador de servicios) deberá acreditarse las normas internas relativas a la propiedad intelectual.

Junto con los aspectos relativos a la propiedad intelectual, no menos importante es el deber de secreto y confidencialidad de la información que los operadores económicos manejan en el marco de la contratación pública en materia de Defensa y Seguridad.

En este punto, la Directiva ya señalaba que, la entidad o el poder adjudicador podrá exigir que la oferta incluya, entre otras cosas, el compromiso del licitador y de los subcontratistas ya identificados de salvaguardar adecuadamente la confidencialidad de toda la información clasificada que posean o que llegue a su conocimiento a lo largo de la duración del contrato y después de la terminación o de la conclusión del contrato, de conformidad con las disposiciones legislativas, reglamentarias y administrativas pertinentes.

El marco jurídico en la normativa española en materia de confidencialidad de la información

En nuestro derecho interno, la Ley 24/2011, de 1 de agosto, de contratos del sector público en los ámbitos de la Defensa y de la Seguridad incorporó a nuestro ordenamiento jurídico las normas contenidas en la Directiva 2009/81/CE, con dos ideas básicas: de una parte, el reconocimiento de que en los contratos relativos a la Defensa y la Seguridad cobra especial relevancia la seguridad en la información que se transmite a los licitadores y la garantía en la continuidad del suministro y, de otra, la necesidad de establecer ciertas normas que faciliten la flexibilidad en los procedimientos de contratación.

Dicha norma tiene por objeto la regulación de la preparación y del procedimiento de adjudicación de los contratos[86] de obras, suministro, servicios y colaboración entre

86 Estos contratos podrán tener por objeto: a) El suministro de equipos militares, incluidas las piezas, componentes y subunidades de los mismos. b) El suministro de armas y municiones destinadas al uso de las Fuerzas, Cuerpos y Autoridades con competencias en seguridad. c) El suministro de equipos sensibles, incluidas las piezas, componentes y subunidades de los mismos. d) Obras, suministros y servicios directamente relacionados con los equipos, armas y municiones mencionados en las letras a), b) y c) anteriores para el conjunto de los elementos necesarios a lo largo de las posibles etapas sucesivas del ciclo de vida de los productos. e) Obras y servicios con fines específicamente militares u obras y servicios sensibles.

el sector público y el sector privado que se celebren en el ámbito de la Defensa y de la Seguridad pública cuando contraten las entidades o poderes adjudicadores que la propia norma determina.

Además en nuestra norma interna se establece la exigencia de que, cuando se trate de contratos públicos que supongan el uso de información clasificada o requieran el acceso a la misma, deberá tenerse en cuenta lo establecido en las disposiciones reglamentarias que dicte la Autoridad Nacional de Seguridad para la Seguridad de la Información Clasificada originada por las partes del Tratado del Atlántico Norte, por la Unión Europea y por la Unión Europea Occidental.

Con independencia de lo anterior, el órgano de contratación deberá tener establecido un órgano de control que será el responsable de la información clasificada a la que el primero pueda tener acceso. Este órgano de control deberá garantizar una adecuada protección de la información clasificada que tenga a su cargo y de la que sea responsable, y velará por el cumplimiento de la normativa de protección de la información clasificada de la Autoridad Nacional para la Seguridad a que se refiere el párrafo anterior.

La acreditación por el candidato o licitador de que dispone de la habilitación correspondiente se realizará por la Autoridad Delegada para la Seguridad de la Información Clasificada designada por Orden PRE/2130/2009, de 31 de julio,. Esta última verificará el grado de la habilitación de seguridad de empresa o, en su caso, de la habilitación de seguridad de establecimiento de que dispone el candidato o licitador. Dicha acreditación deberá realizarse con anterioridad al momento en que sea necesario tener acceso a la información clasificada y, en todo caso, con anterioridad a la adjudicación del contrato.

En el caso de candidatos o licitadores no nacionales, le corresponderá a la Autoridad Delegada para la Seguridad de la Información Clasificada reconocer, al amparo de la normativa internacional vigente, las habilitaciones expedidas por otros Estados, así como certificar al órgano de contratación dicha circunstancia.

En todo caso es preciso puntualizar que, en el año 2006 el legislador fue consciente de que la situación normativa de seguridad de la información en el Ministerio de Defensa era compleja, "debido a la gran cantidad de normativa existente, a las diferentes procedencias, a la coexistencia de normativa obsoleta con normativa moderna y a la falta de un tronco común que facilite el desarrollo normativo coordinado".

Fruto de dicha reflexión nació la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa. Esta norma define una estructura funcional de responsabilidades en la protección de la información, bajo la autoridad del director de Seguridad de la Información, cargo correspondiente al secretario de Estado de Defensa.

La política señala además los tres pilares básicos sobre los que se debe sustentar la seguridad de la información: organizativo, técnico y normativo. En torno a ellos se desarrollan las distintas medidas enfocadas a preservar la confidencialidad, integridad y disponibilidad de la información, en todos los ámbitos.

Posteriormente mediante la Orden DEF/2524/2012, de 8 de noviembre, por la que se adecúan las normas y medidas de seguridad de la información del Ministerio de Defensa en poder de las empresas, aclaró el marco normativo de la seguridad de la información en poder de las empresas relacionadas con el Ministerio de Defensa tras la entrada en vigor de la Ley 24/2011, de 1 de agosto, indicando que, la seguridad de la información del Ministerio de Defensa en poder de las empresas se regirá por lo establecido en la Ley 24/2011, de 1 de agosto, de contratos del sector público en los ámbitos de la Defensa y de la Seguridad y por lo dispuesto en el apartado séptimo. 5 de la Política de la Seguridad de la Información del Ministerio de Defensa aprobada por la Orden Ministerial 76/2006.

En la clasificación de la información realizada por la Orden Ministerial 76/2006 contempla la siguiente estructura:

- Se consideran MATERIAS CLASIFICADAS los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la Seguridad y Defensa del Estado. Estas "materias clasificadas" serán exclusivamente las que, se definen posteriormente como "secreto y reservado".

- Se consideran MATERIAS OBJETO DE RESERVA INTERNA los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pudiera afectar a la seguridad del Ministerio de Defensa, amenazar sus intereses o dificultar el cumplimiento de su misión. Estas materias son las que posteriormente se definen como CONFIDENCIAL y DIFUSIÓN LIMITADA.

Las "materias clasificadas" y las "materias objeto de reserva interna" quedan englobadas en el concepto general de INFORMACIÓN CLASIFICADA[87].

En relación con los GRADOS DE CLASIFICACIÓN estos se dividen en los siguientes:

87 La clasificación es el acto formal mediante el cual, a una determinada información, se le asigna un grado en atención a las medidas de seguridad que requiere frente a la pérdida de confidencialidad y se emplea para poner en conocimiento del receptor o depositario de la información la necesidad de protegerla y el grado de protección requerido. La reclasificación es la asignación de un nuevo grado de clasificación a una información clasificada. La desclasificación es el acto formal mediante el cual se anula de manera expresa la clasificación de una información. Este acto formal no será necesario si la autoridad que otorgó la clasificación señaló un plazo de duración de ésta, o las circunstancias que lo condicionen.

- SECRETO (S): se aplica a los asuntos, actos, documentos, informaciones, datos y objetos que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada por autoridad competente para ello pudiera dar lugar a riesgos o perjuicios de la Seguridad y Defensa del Estado.
- RESERVADO (R): se aplicar a los asuntos, actos, documentos, informaciones, datos y objetos no comprendidos en el apartado anterior por su menor importancia, pero cuyo conocimiento o divulgación pudiera afectar a la Seguridad y Defensa del Estado.
- CONFIDENCIAL (C): se aplica a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera dañar la seguridad del Ministerio de Defensa, perjudicar sus intereses o dificultar el cumplimiento de su misión.
- DIFUSIÓN LIMITADA (DL): se aplica a los asuntos, actos, documentos, informaciones, datos y objetos, no comprendidos en los apartados anteriores, cuya revelación no autorizada pudiera ir en contra de los intereses y la misión del Ministerio de Defensa.

La facultad para clasificar de SECRETO o RESERVADO corresponde a las autoridades y órganos establecidos en el artículo cuatro de la Ley 9/1968, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre sobre secretos oficiales, no pudiendo ser transferida ni delegada.

La facultad para clasificar de CONFIDENCIAL o DIFUSIÓN LIMITADA, corresponde, en el ámbito de su competencia, a las siguientes autoridades: Ministro de Defensa. Jefe del Estado Mayor de la Defensa. Secretario de Estado de Defensa. Secretario de Estado Director del CNI. Subsecretario de Defensa. Secretario General de Política de Defensa. Jefe del Estado Mayor del Ejército. Jefe del Estado Mayor de la Armada. Jefe del Estado Mayor del Ejército del Aire. Estas autoridades pueden delegar oficialmente dicha atribución.

En relación con la INFORMACIÓN NO CLASIFICADA, dependiendo de su ámbito de distribución, podrá ser: Información de USO OFICIAL: información cuya distribución esté limitada al ámbito del Ministerio de Defensa, o a personas y organismos que desempeñen actividades relacionadas con el mismo. Información de USO PUBLICO: información cuya distribución no esté limitada.

Las áreas en que se divide la seguridad de la información, atendiendo al elemento tangible que hace uso de ella, ya sea elaborándola, presentándola, almacenándola, procesándola, transportándola o destruyéndola son, de acuerdo con la Orden Ministerial 76/2006:

- Seguridad de la Información en las Personas.
- Seguridad de la Información en los Documentos.

- Seguridad de la Información en los Sistemas de Información y Telecomunicaciones.
- Seguridad de la Información en las Instalaciones.
- Seguridad de la Información en poder de las Empresas.

Parece que legalmente la problemática de la confidencialidad y deber de secreto de la información, al menos formalmente, está resuelta.

Las leyes señalan procedimientos, clasifican la información y establecen las obligaciones de los sujetos que la manejan. No obstante y pese a ello, como veremos más adelante, puede que todo esto sea insuficiente a la luz del momento social en que nos encontramos.

El marco jurídico en la normativa española en materia de propiedad intelectual

Volviendo a la Ley 24/2011 parece que ésta transpone fielmente las disposiciones de la Directiva, con cierto detalle en la regulación del deber de secreto y confidencialidad de la información y datos que se manejen por el licitador y adjudicatario, pero no incorpora (como tampoco lo hizo la Directiva 2009/81/CE) las reglas a tener en cuenta en relación con los derechos de propiedad intelectual derivados de las obras o servicios realizados en relación con las actividades de la Defensa y de la Seguridad Pública.

Esta cuestión es relevante si tenemos en cuenta que, con las tecnologías y más concretamente con el desarrollo de sofisticados algoritmos, se está impulsando un rápido incremento en las capacidades autónomas de sistemas, tanto de ataque como de defensa, como aviones no tripulados, vehículos de auto-conducción, robots y otros sistemas que cada vez desempeñan un papel más importante en los conflictos bélicos.

Las armas inteligentes de ataque y defensa, cuya dependencia del control humano (al menos directo) es cada vez menor, se van incorporando a los "arsenales" de los distintos Estados e incluso están modificando las estrategias y tácticas de guerra.

De hecho, las tecnologías y las comunicaciones han propiciado que muchas operaciones de asedios u ofensivas en campos de combate ya no requieran de la intervención humana de forma directa, siendo el resultado de un proceso informático cuya decisión ha sido adoptada por un algoritmo.

Podríamos decir que estos algoritmos tienen un precio de mercado y hemos pasado de "vender armas de guerra tangibles a algoritmos informáticos intangibles" sometidos a derechos de propiedad intelectual e industrial.

¿Pero de quién son estos algoritmos? ¿A quién corresponde la titularidad de las aplicaciones y desarrollos informáticos que dichos algoritmos recrean?

Aunque pudiera parecer que los derechos de propiedad sobre las aplicaciones informáticas y los algoritmos que se desarrollan en el ámbito de la Defensa y la Seguridad son del poder adjudicador que contrata la obra o el servicio, lo cierto es que a falta de disposiciones especiales en esta materia debemos acudir al Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia (en adelante TRLPI) .[88]

El TRLPI es el resultado de una serie de reformas en materia de propiedad intelectual hacía la búsqueda constante del equilibrio entre la evolución de los medios de explotación de las obras protegidas, los derechos de sus autores y otros titulares y el acceso por terceros a aquellas.

Entre las obras protegidas el TRLPI incluye a los programas de ordenador entendidos como toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación. A los mismos efectos, la expresión programas de ordenador también comprende su documentación preparatoria, técnica y manuales de uso.

Hay que tener en cuenta que el sector de la Defensa hace un uso intensivo de la tecnología, y su investigación y desarrollo de vanguardia tienen efectos indirectos en otros ámbitos como el de la electrónica, las tecnologías de la información y la comunicación, el transporte, la biotecnología y la nanotecnología. De hecho, muchas de las tecnologías desarrolladas para el sector de la Defensa se han convertido en motores del crecimiento en sectores civiles, como el posicionamiento global, internet o la observación de la tierra. Pero poco a poco, esto se ha ido convirtiendo en un proceso de ida y vuelta, ya que los sectores civiles también contribuyen a la Defensa fundamentalmente en con el desarrollo de software.

Cada vez es más difícil definir el sector, ya que los límites entre Defensa, Seguridad y tecnologías civiles (como la electrónica o las telecomunicaciones) están haciéndose menos precisos, pero ello no debería hacer que se descuide la negociación de los derechos de propiedad intelectual de las aplicaciones y desarrollos informáticos cuando éstos sean el objeto de la prestación de un servicio, obra o suministro de equipos, armas y municiones militares.

88 Este texto refundido es consecuencia del cumplimiento del mandato legal de la disposición final segunda de la Ley 27/1995, de 11 de octubre, de incorporación al Derecho español de la Directiva 93/98/CEE, del Consejo, de 29 de octubre, relativa a la armonización del plazo de protección del derecho de autor y de determinados derechos afines, a través de la cual se autorizó al Gobierno para que, antes del 30 de junio de 1996, aprobara un texto que refundiese las disposiciones legales vigentes en materia de propiedad intelectual, regularizando, aclarando y armonizando los textos que hubieran de ser refundidos.

Visto este flujo de información y tecnología entre el sector civil y el sector militar, parece que cobra importancia el tema de la propiedad intelectual y la posible explotación del software desarrollado para uno u otro sector, con fines ajenos a aquellos que originaron la creación. Si atendemos a las leyes, la obra, el resultado del proceso creador, es de quien la elabora. De acuerdo con el TRLPI, los programas de ordenador se constituyen como obras literarias (aunque pueda parecer inexplicable) y la propiedad intelectual de una obra literaria corresponde al autor por el solo hecho de su creación.

La protección de todos los derechos de propiedad sobre la obra para su autor, nace desde el mismo momento de la creación de aquella sin que sea necesario que se den otros requisitos, ni aún si quiera, la inscripción o registro de la obra en ningún organismo ni público ni privado. Para que la obra sea protegible por las normas de propiedad intelectual es requisito imprescindible que la misma sea original y esté expresada por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro.

Ello implica que, tal y como se reconoce en el artículo 9 recogido en las "Normas relativas a la existencia, alcance y ejercicio de los derechos de propiedad intelectual" del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), la protección del derecho de autor abarca las expresiones pero no las ideas.[89]

Atendiendo al TRLPI será considerado autor de una aplicación informática o programa de ordenador, la persona natural que lo crea. Sin perjuicio de lo anterior, de la protección que el TRLPI concede al autor se pueden beneficiar las personas jurídicas en los casos expresamente previstos en el propio TRLPI consistentes básicamente en la llamada "obra colectiva"[90] y la obra elaborada bajo "relación laboral".[91] La pregunta que cabe realizarse es, en qué manera.

89 En el mismo sentido, el artículo 2 "ámbito de la protección del derecho de autor" del Tratado de la OMPI sobre Derecho de Autor: *La protección del derecho de autor abarcará las expresiones pero no las ideas, procedimientos, métodos de operación o conceptos matemáticos en sí.*

90 De acuerdo con el TRLPI se considera obra colectiva la creada por la iniciativa y bajo la coordinación de una persona natural o jurídica que la edita y divulga bajo su nombre y está constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada. En este caso, salvo pacto en contrario, los derechos sobre la obra colectiva corresponderán a la persona que la edite y divulgue bajo su nombre.

91 El TRLPI considera "obra laboral", aquella obra creada en virtud de una relación laboral. En el caso de la creación de programas de ordenador, si éstos son creados por un trabajador asalariado en el ejercicio de sus funciones o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario.

Para que podamos aplicar con total seguridad jurídica la premisa anterior, es decir, que el encargo de creación de un programa de ordenador sea titularidad del cualquier órgano o entidad pública, será preciso que los pliegos o documentos contractuales que se utilicen al efecto sean inequívocos en su redacción.

Esto implica que en la contratación de desarrollos informáticos por parte de los órganos correspondientes en materia de Seguridad y Defensa se señale expresamente en los pliegos administrativos de contratación a quién corresponderá la propiedad de la obra (programas informáticos o algoritmos) con independencia de quién sea su autor material.

Dicho de otra forma, será preciso determinar que el autor material (ya se trate de una persona natural o varias o ya se trate de una persona jurídica), cederá la propiedad intelectual de la obra (programa de ordenador o algoritmos) objeto de contratación, al poder adjudicador.

También cabrían otras opciones como compartir la propiedad distinguiendo los ámbitos temporales, geográficos y modalidades de explotación. Pero igualmente deberían ser indicadas en el contrato o en los pliegos de contratación.

La llamada "propiedad intelectual" está compuesta por dos tipos de derechos en relación con los programas de ordenador o software: los llamados derechos morales sobre la obra (como por ej. la paternidad de la misma) los cuales son personalísimos, no son negociables ni transmisibles y pertenecerán siempre al autor hasta su fallecimiento.

Y los llamados derechos económicos o de explotación que son: el de reproducción, transformación y distribución de la obra, los cuales sí son transmisibles.

Pero que la transmisión de los derechos económicos o de explotación pueda llevarse a efecto, el TRLPI prevé expresamente que esta deberá llevarse a cabo por escrito entre las partes contratantes, con indicación de (i) si la cesión se efectúa en exclusiva[92] o no, (ii) el derecho o derechos cedidos, (iii) las modalidades de explotación expresamente previstas, (iv) el tiempo y (vii) el ámbito territorial de la cesión.

A falta de pacto escrito sobre los extremos anteriores, la ley entiende que:

a) La falta otorgamiento de la cesión exclusiva indica que no tendrá este carácter.

b) La falta de mención del tiempo limita la transmisión a cinco años.

c) La falta del ámbito territorial limita la cesión al país en el que se realice la cesión.

92 La cesión en exclusiva deberá otorgarse expresamente con este carácter y atribuirá al cesionario, dentro del ámbito de aquélla, la facultad de explotar la obra con exclusión de otra persona, comprendido el propio cedente, y, salvo pacto en contrario, las de otorgar autorizaciones no exclusivas a terceros. Asimismo, le confiere legitimación con independencia de la del titular cedente, para perseguir las violaciones que afecten a las facultades que se le hayan concedido.

d) Si no se expresan específicamente y de modo concreto las modalidades de explotación de la obra, la cesión quedará limitada a aquella que se deduzca necesariamente del propio contrato y sea indispensable para cumplir la finalidad del mismo.

Todo lo anterior indica que, estas previsiones deberían ser tenidas en cuenta en los pliegos de contratación en materia de Defensa y Seguridad, así como el hecho de que de acuerdo con la normativa de propiedad intelectual, será nula cualquier cesión de derechos de explotación que realice el autor o desarrollador respecto del conjunto de las obras que pueda crear el autor en el futuro así como las estipulaciones por las que el autor se comprometa a no crear alguna obra en el futuro.

Vinculado a lo anterior, hay que establecer cuál es la remuneración que se efectúa al autor por la cesión de los derechos.[93]

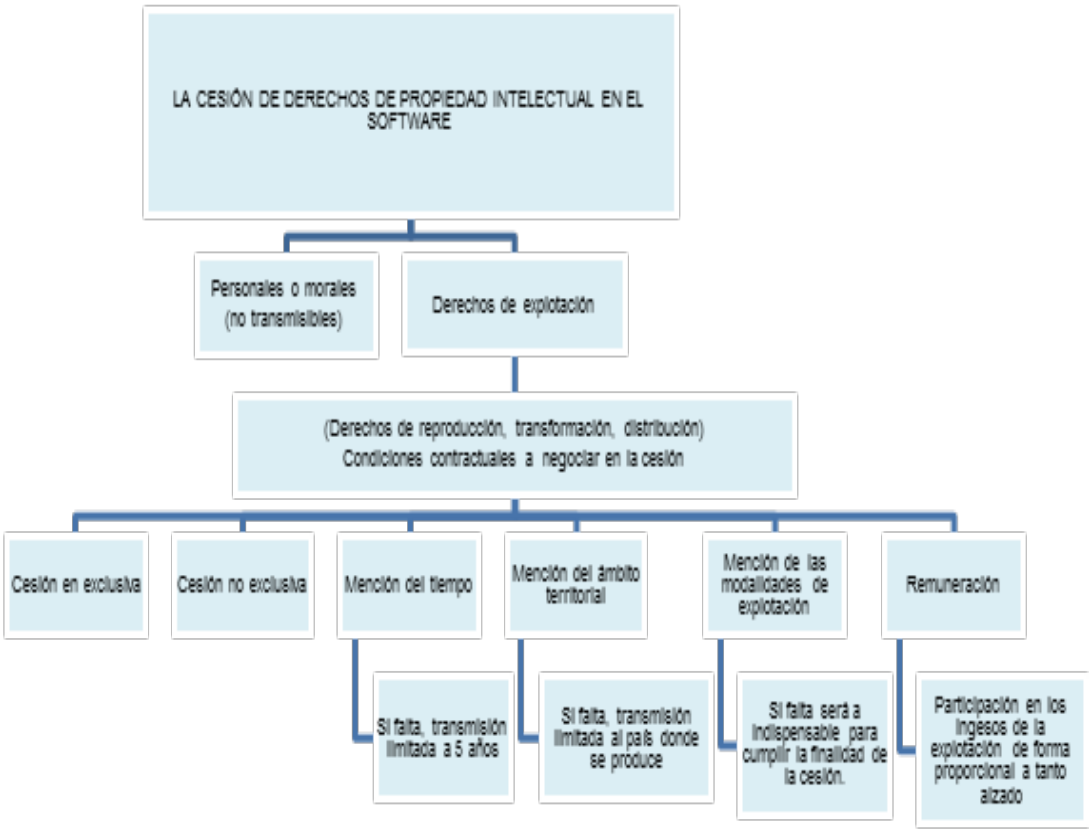
A priori la norma general es que la cesión otorgada por el autor a título oneroso le confiere una participación proporcional en los ingresos de la explotación, en la cuantía convenida con el cesionario. No obstante, puede estipularse una remuneración "a tanto alzado" para el autor en determinados casos.

Pero si en la cesión a tanto alzado se produjese una manifiesta desproporción entre la remuneración del autor y los beneficios obtenidos por el cesionario, el TRLPI faculta al autor para pedir la revisión del contrato y, en defecto de acuerdo, acudir al Juez para que fije una remuneración equitativa, atendidas las circunstancias del caso.

También es importante advertir que, respecto de los soportes materiales donde se incorpore la obra objeto de contratación (por ej. el software) debe tenerse en cuenta que, con la transmisión de los derechos sobre el intangible el adquirente no adquiere la propiedad del soporte a que se haya incorporado la obra "*per se*", de forma que, será preciso en cualquier documentación contractual incluir las previsiones de la cesión de los derechos de propiedad, tanto del programa de ordenador como del/os soportes donde se encuentre incorporado.

Como conclusión simplemente advertir que en el sector de la Defensa como en otros sectores, el valor de lo intangible empieza a cobrar más importancia que el valor de lo tangible, y es importante tener los requisitos regulatorios que garantizan la propiedad de aquella tecnología que presumiblemente nos dará una ventaja competitiva o en otros casos, la independencia tecnológica de los proveedores.

93 Partimos del hecho de que la ley de propiedad intelectual pretende que los autores puedan vivir de sus creaciones y de la explotación comercial que de las mismas se realice.



Cuadro esquemático de la transmisión de derechos de propiedad intelectual sobre los programas de ordenador.

Una reflexión sobre los principios éticos y morales en el tratamiento de la información

Merece la pena hacer una reflexión acerca de la influencia y el cambio social que las tecnologías han causado a nivel global y cómo ello ha influido en el tratamiento de la información y la consideración ética, que de su uso se tiene.

Si los apartados anteriores veíamos los esfuerzos realizados por la Unión Europea y por nuestra normativa interna, en procurar la seguridad y la confidencialidad de la información, no hay que olvidar que en ocasiones., es únicamente el deber de secreto, es decir, la conciencia individual de las personas, lo que garantizará la confidencialidad de los datos e informaciones.

Pero quizás podríamos decir que ha sido precisamente la rápida evolución y por qué no, la disrupción de las tecnologías en casi todos los ámbitos, lo que ha propiciado una crisis de valores de los individuos y de las sociedades.

Quizás los casos Snwoden[94] y Manning[95] (wikileaks) son un paradigma de ello. Ambos fueron los protagonistas de la comisión de ilícitos jurídicos en relación con la revelación de información protegida, pero bajo la convicción ética de estar haciendo no sólo lo correcto, sino un bien para la sociedad.

Las claves de estos casos, que al objeto de este análisis nos interesan, son dos: en primer lugar, la evidencia de que el deber de sigilo es un deber personal e individual que depende de la conciencia del individuo obligado a guardarlo, de forma que, pese al establecimiento de medidas técnicas organizativas o de cualquier otra naturaleza, la información objeto de custodia sólo estará segura si quien tiene derechos de acceso y uso también es consciente de la necesidad de su salvaguarda o tiene la convicción ética de esta necesidad. Y en segundo lugar, la evidencia de que socialmente los conceptos de privacidad e intimidad han cambiado.

Como hemos manifestado, Edward Snowden, éticamente entendió que con sus declaraciones hacía bien a la sociedad y antepuso esta convicción a la transgresión de sus deberes de sigilo. Una gran parte de la sociedad apoyó esta postura.

El caso Snwoden puso en jaque a la Unión Europea que, se vio obligada abrir una serie de investigaciones que llevaron a la aprobación de la "Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EEUU, los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la Unión Europea y en la cooperación transatlántica en materia de justicia y asuntos de interior".

La Unión Europea no pudo acallar las voces de aquellos que se preguntaban si la situación creada por las revelaciones de Edward Snowden constituían el indicio de un giro social "en bloque" hacia la aceptación del fin de la intimidad a cambio de seguridad.

Los ciudadanos se preguntaban si nos enfrentamos a una violación de la intimidad de tal magnitud que no sólo los criminales, sino las empresas de telecomunicaciones y las agencias de inteligencia saben todos los detalles de sus vidas y si esto era un hecho que tenemos que aceptar "sin más discusión" o es responsabilidad del legislador adaptar las políticas y las herramientas legales a su disposición para limitar los riesgos y evitar mayores perjuicios en caso de que fuerzas menos democráticas accediesen al poder.

94 Edward Snowden trabajó para la CIA y la Agencia Nacional de Seguridad y en la actualidad está acusado de espionaje por los EE UU tras revelar dos programas de espionaje secretos que permitían a la inteligencia estadounidense registrar datos de llamadas en EEUU y acceder a servidores de las principales compañías de Internet para buscar conexiones con el terrorismo internacional.

95 El soldado Bradley Manning, detenido el 26 de mayo de 2010 en Irak, acusado de sustraer documentos de las redes secretas del Pentágono y entregárselos a Wikileaks.

El debate sobre la vigilancia masiva, no tuvo lugar de forma uniforme dentro de la Unión Europea y aún menos, fuera de sus fronteras.

La Comisión LIBE[96] inició una investigación y pudo escuchar valiosas contribuciones de los organismos parlamentarios de control de algunos Estados miembros (Bélgica, los Países Bajos, Dinamarca e incluso Noruega) pero otros sin embargo (los parlamentos británico y francés) rechazaron la participación.

Se puso de manifiesto que nos encontramos ante nuevo escenario: Los grandes proveedores de servicios de internet vigilan las comunicaciones electrónicas, conocen nuestros secretos y acopian nuestra información. Estas empresas aglutinan en sus sistemas más información de la que uno mismo pudiera llegar a tener, llegando incluso a poder crear perfiles y segmentaciones de las personas, en relación con sus aspectos psicológicos, hábitos de consumo, hábitos de navegación o personalidad.

Esta información sirve a dichos proveedores para monetizar sus servicios llegando, entre otros, a acuerdos publicitarios a través de los cuales la publicidad personalizada se vende a un precio muy alto. Y además, los hechos constaron que la información también puede ser compartida con los gobiernos.

En este aspecto nos encontramos además en el diferente régimen de protección de la información sobre las personas de la Unión Europea frente a EEUU u otros terceros países donde ésta no existe o no tiene las garantías contempladas en Europa. A ello hay que añadir que, la llamada Ley Patriota, (USA PATRIOT Act)[97] aprobada tras los atentados del 11 de septiembre persigue combatir al terrorismo dotando a las distintas agencias de seguridad estadounidenses de mayores poderes de vigilancia, lo cual propició el hecho de que las Agencias de Seguridad americanas pudieran acceder de todos los datos que manejan los grandes proveedores de internet.

La Comisión LIBE tuvo que resolver su conflicto acerca de si Europa debía actuar frente a los hechos acaecidos en EEUU o no.

Entre las razones para no actuar:

- El hecho de que no incide en al ámbito de competencias de la Unión Europea por tratarse de temas de Seguridad Nacional. Las revelaciones de Edward Snowden

96 La Comisión de Libertades Civiles, Justicia y Asuntos de Interior es responsable de la protección, dentro del territorio de la Unión Europea, de los derechos de los ciudadanos, los derechos humanos y los derechos fundamentales, incluida la protección de las minorías, establecidos en los Tratados y en la Carta de los Derechos Fundamentales de la Unión Europea. Se ocupa de las cuestiones relacionadas con la protección de datos de carácter personal. Asimismo se ocupa de las normas relativas a la migración y el asilo, la gestión integrada de las fronteras exteriores, así como la cooperación policial y judicial en materia penal. http://www.eppgroup.eu/es/libe.

97 Recientemente discutida en el Senado de los Estados Unidos con el fin de analizar su prórroga y en qué forma así como la necesidad de llevar a cabo su reforma.

están relacionadas con las actividades de los servicios de inteligencia de Estados Unidos y de algunos de los Estados miembros, pero la Seguridad Nacional es una competencia nacional, por lo que la Unión Europea no tiene competencias en dichos asuntos y no es posible emprender acciones a nivel comunitario.

- Cualquier seguimiento de estas revelaciones, o su mera consideración, debilita aún más la seguridad de Estados Unidos y de la Unión Europea, ya que no condena la publicación de documentos cuyo contenido, incluso redactado tal y como explican los medios de comunicación, puede poner una valiosa información en manos de grupos terroristas.
- La falta de legitimidad de los denunciantes de irregularidades. Estados Unidos y Reino Unido pusieron de manifiesto que cualquier debate iniciado o acción prevista a partir de las revelaciones de Edward Snowden son intrínsecamente sesgados e irrelevantes, ya que se basan en un acto inicial de traición.
- Aunque se confirmasen errores y actividades ilegales, deben ponderarse frente a la necesidad de mantener las relaciones especiales entre Estados Unidos y Europa para conservar los intereses económicos, comerciales y de asuntos exteriores comunes. Hay que confiar en el Gobierno Los gobiernos de Estados Unidos y de la Unión Europea se eligen de forma democrática.

Entre las razones para actuar:

- El postulado de la vigilancia masiva: ¿en qué sociedad queremos vivir?. La Unión Europea manifestó que, desde los ataques del 11 de septiembre de 2001, el protagonismo de la seguridad y el cambio hacia una vigilancia específica ha dañado y socavado el concepto de la intimidad.
- La vigilancia masiva e indiscriminada amenaza los derechos fundamentales de los ciudadanos, como el derecho a la intimidad, la protección de datos, la libertad de prensa o un juicio justo, todos ellos consagrados internacionalmente. Estos derechos no pueden burlarse ni negociarse por posibles ventajas a cambio, a menos que así esté dispuesto en instrumentos legales y de conformidad con los tratados.
- Las competencias nacionales en cuestiones de inteligencia y seguridad nacional no excluyen una competencia paralela de la Unión Europea.
- Aunque los servicios de inteligencia llevan a cabo una función indispensable en la protección frente a las amenazas internas y externas, tienen que actuar dentro de los límites del Estado de derecho, y, para ello, tienen que estar sometidos a un estricto y exhaustivo mecanismo de control.
- Las revelaciones de Edward Snowden y las posteriores publicaciones en los medios de comunicación han destacado el papel crucial de la prensa en una democracia para garantizar la rendición de cuentas de los gobiernos. Cuando

los mecanismos de supervisión no evitan ni corrigen la vigilancia masiva, es muy importante el papel de los medios de comunicación y los denunciantes de irregularidades al desvelar posibles ilegalidades o abusos de poder.

En definitiva la Unión Europea se vio obligada a elegir entre una "política de statu quo", hay suficientes razones para no actuar, esperar y ver, y una "política de evaluación de la realidad", la vigilancia no es nueva, pero hay pruebas suficientes de una escala sin precedentes en el alcance y la capacidad de las agencias de inteligencia que hacen preciso que la Unión Europea actúe.

Aunque a criterio de la Unión Europea, la Ciberseguridad solo puede resultar positiva y eficaz si se basa en los derechos fundamentales y las libertades enunciados en la Carta de los Derechos Fundamentales, y en particular si se cumple la normativa de protección de datos que la propia Unión Europea ha establecido, la realidad es que esta normativa ha quedado obsoleta y Europa no se pone de acuerdo en cómo debe llevarse a cabo su actualización.

Las investigaciones de la Comisión LIBE así la resolución que por votación de los Estados Miembros se aprobó,[98] Resolución del Parlamento Europeo, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EEUU, los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la Unión Europea y en la cooperación transatlántica en materia de justicia y asuntos de interior, pusieron de manifiesto, que:

- Para la Unión Europea los derechos fundamentales, entre otros la libertad de expresión, de prensa, de conciencia, de religión y de asociación, la vida privada y la protección de datos, constituyen piedras angulares de la democracia, incompatibles con la vigilancia masiva de seres humanos.
- La transferencia de datos personales de los ciudadanos de la Unión Europea a terceros Estados está sometida a férreas normas y procedimientos quedando limitada a organizaciones que han "autocertificado" su adhesión a los principios de la Directiva Europea de Protección de Datos pero cuya situación claramente no está actualizada, lo que significa que la empresa no cumple los requisitos de puerto seguro aunque continúe recibiendo datos personales de entidades ubicadas en países miembros de la Unión Europea.
- Que las instituciones y Estados miembros de la Unión Europea deben promover el «Habeas corpus digital europeo proteger los derechos fundamentales en una era digital» con un "paquete de acciones" al efecto.

98 Resolución completa en http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=ES&ring=A7-2014-0139.

En esta línea nos preguntamos sí en un entorno tan cambiante como es el del Ciberespacio tiene sentido aplicar una norma con veinte años de antigüedad. La respuesta obviamente es negativa.

La Directiva de protección de datos de 1995 fue un instrumento legislativo básico para la protección de los datos personales en Europa, marcó un hito en la historia de la protección de datos. Sus objetivos, asegurar el funcionamiento del mercado único y la protección efectiva de los derechos y las libertades de los ciudadanos, siguen siendo válidos pero el entorno ha cambiado. La Directiva se adoptó y sirvió en un momento en que internet estaba aún en una fase incipiente.

En el nuevo y complejo entorno digital actual, las normas vigentes no aportan ni el grado de armonización requerido ni la eficacia necesaria para preservar el derecho a la protección de datos personales.

Había consenso unánime por los Estados miembros en la necesidad del cambio y con el fin de preparar la reforma del marco jurídico de protección de datos de la Unión Europea, esta ha organizado, desde 2009, varias rondas de consultas públicas y ha entablado un diálogo intensivo con los interesados.

Estas conversaciones dejaron claro que tanto los ciudadanos como las empresas deseaban que la Comisión Europea procediese a una reforma general de las normas de protección de datos de la Unión Europea y tras evaluar las repercusiones de las distintas opciones, la Comisión Europea decidió proponer un nuevo escenario legal a través de un Reglamento (que sustituya a la Directiva de protección de datos) en el que se fije el marco jurídico general de protección de datos de la UE.

Pero los trabajos avanzan muy lentamente fruto de las considerables divergencias entre las posiciones regulatorias de los distintos Estados miembros.

En la actualidad Europa tiene un entorno jurídico fragmentado que ha generado inseguridad jurídica y protección desigual de las personas físicas. Además, ha generado costes innecesarios y cargas administrativas para las empresas y actúa como desincentivo para aquellas que operan en el mercado único y desearían expandir sus operaciones a otros terceros países.

Europa no se pone de acuerdo para alcanzar una posición común sobre este asunto, que constituye un pilar básico de la nueva era digital.

ROBOTS, SISTEMAS AUTÓNOMOS Y ARMAS INTELIGENTES

La carrera por el incremento de las capacidades autónomas con sistemas no tripulados, chips insertados en el cuerpo de los soldados, herramientas de geolocalización, programas de toma de decisiones automáticos, robots y otros sistemas de armas

autónomas, junto con el uso de otras tecnologías disruptivas como microondas, están desafiando a las leyes naturales y a las leyes de los Estados.

Por buscar algún símil, podríamos decir que la ingeniería genética nos lleva ventaja en el establecimiento de iniciativas institucionales y de otro orden para evaluar, y en su caso regular, la tecnología aplicada a las leyes de la salud humana.

De hecho, el progreso en este campo ha ido acompañado de la creación obligatoria de organismos, comités consultivos y comisiones éticas y bioéticas así como de la conducta de los individuos, todos ellos destinados a evaluar los problemas éticos que en el campo de la medicina e investigación esta nueva rama de la Medicina iba provocando.

Pero en la carrera armamentística por las armas inteligentes, parece que ya llegamos tarde. La creencia de que el uso de armamento inteligente tiene menos coste en vidas humanas, por ser más selectivo y no requerir el enfrentamiento físico de los combatientes, según algunas voces, incrementa el número de conflictos.

El Centro para una Nueva Seguridad Estadounidense (CNAS) ha puesto en marcha un proyecto sobre ética de Autonomía, con el fin de examinar los aspectos jurídicos, morales, y éticos, del incremento en las capacidades de los Estados de las armas autónomas[99] que dará lugar a una serie de documentos que servirán de ayuda a los Estados, expertos, abogados, académicos y militares para evaluar y analizar los problemas que plantean las armas autónomas.

En este sentido, el Consejo de Derechos Humanos de Naciones Unidas ya puso de manifiesto[100] que *los robots autónomos letales son sistemas de armas que, una vez activados, pueden seleccionar y atacar objetivos sin necesidad de intervención humana. Dan lugar a graves cuestiones relacionadas con la protección de la vida en tiempos tanto de guerra como de paz, a saber, entre otras, la medida en que se pueden programar para cumplir las prescripciones del derecho internacional humanitario y las normas del derecho internacional de los derechos humanos relativas a la protección de la vida.*

Por otra parte, su despliegue puede ser inaceptable porque no es posible establecer un sistema adecuado de responsabilidad jurídica y porque los robots no deben tener el poder de decidir sobre la vida y la muerte de seres humanos.

99 Para más información http://www.cnas.org/ethicalautonomy.

100 Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo: Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Christof Heyns, 9 abril de 2013. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_sp.pdf.

En su informe, el Relator Especial[101] recomendó a los Estados el establecimiento de moratorias nacionales sobre determinados aspectos de los robots autónomos letales, e instó a que se establezca un grupo de alto nivel sobre esos dispositivos encargado de articular una política de la comunidad internacional sobre la cuestión

Además en el informe ya se indicó que *los robots a menudo se describen como máquinas que se basan en el paradigma detección-pensamiento-acción: tienen sensores que les proporcionan cierto grado de conciencia de la situación; procesadores o inteligencia artificial que "deciden" cómo responder a un estímulo determinado; y efectores que ejecutan esas "decisiones". En el panorama contemplado actualmente, los seres humanos seguirán al menos formando parte de lo que podría considerarse el control más amplio: programarán los objetivos finales en los sistemas robóticos y tomarán la decisión de activarlos y, en caso necesario, desactivarlos, mientras que las armas autónomas traducirán esos objetivos en tareas y las ejecutarán sin necesidad de una nueva intervención humana. Pero la plena autonomía acabará significando seguramente que, en un plazo de diez años, una participación del ser humano inferior a la actual.*

Estamos de acuerdo con el autor del informe con el hecho de que surgen muchos interrogantes y además añadimos la pregunta sobre, en qué medida el marco jurídico existente es suficiente para regular el supuesto de despliegue de robots autónomos con combatientes humanos o incluso, el despliegue de aquellos sin ninguna contraparte humana.

Como hemos visto en apartados anteriores, desde el punto de vista de la fabricación de la tecnología, y concretamente en el campo de la robótica, existe una cooperación continua entre las tecnologías militares y las no militares, lo cual dificulta su regulación y no es fácil establecer criterios inequívocos.

Las mismas plataformas robóticas pueden tener aplicaciones tanto civiles como militares y pueden desplegarse con fines no letales (por ejemplo, para desactivar artefactos explosivos improvisados) o poseen capacidad letal (es decir, robots autónomos letales).

No menos importante es la cuestión planteada por el Relator Especial en su informe de Naciones Unidas al indicar que *además de los esfuerzos realizados en los últimos años por el derecho internacional a fin de reducir los conflictos armados y para que el uso de la fuerza durante las operaciones de mantenimiento del orden fuera un último recurso, hay otros elementos inherentes al ser humano que le inducen a no entrar en guerra o no recurrir al uso de la fuerza que siguen desempeñando un papel importante, como son la aversión a perder la vida, a perder seres queridos o a tener que matar a otras personas.*

101 El título de Relator Especial es un título otorgado a los individuos que trabajan en representación de las Naciones Unidas y que cumplen con el mandato específico otorgado por la ex Comisión de Derechos Humanos de la ONU de investigar, supervisar y sugerir soluciones para los problemas de derechos humanos en países y territorios determinados (mandatos por país), o violaciones específicas a los derechos humanos en todo el mundo (mandatos temáticos).

Pero la distancia física y psicológica respecto del empleo efectivo de fuerza consiguiente a la introducción de robots autónomos letales puede atenuar esas tres preocupaciones e incluso hacerlas imperceptibles para quienes estén del lado del Estado que las despliegue. Los jefes militares, por ejemplo, pueden por tanto estar más dispuestos a desplegar esos robots que soldados reales. Y esa facilidad podría influir en las decisiones políticas. Debido al bajo o menor costo en vidas humanas durante los conflictos armados para los Estados que posean tales robots en sus arsenales, la opinión pública nacional podría, con el tiempo, mostrarse cada vez más desinteresada y dejar que la decisión de emplear la fuerza se convierta en gran parte en una cuestión económica o diplomática para el Estado, lo que supondría la "normalización" de los conflictos armados.

En definitiva según este planteamiento, los robots autónomos letales podrían rebajar el umbral exigido para que un Estado entre en guerra o emplee otra forma de fuerza letal, de modo que el conflicto armado dejaría de ser una medida de último recurso.

Por otro lado, parece que hay opiniones que aseguran que los robots autónomos también pueden cumplir las exigencias del derecho internacional humanitario en los campos de batalla, lo cual en todo caso tampoco sería fácil.

De hecho, Naciones Unidas plantea en su informe que, *en las situaciones en que los robots autónomos letales no puedan distinguir claramente entre los combatientes u otros beligerantes y los civiles, su empleo será ilegal. E indica que es probable que varios factores impidan que los robots funcionen de conformidad con esas normas: falta de idoneidad tecnológica de los sensores existentes, incapacidad para comprender el contexto, y dificultad de aplicar términos del derecho internacional humanitario para definir el estatuto de no combatiente en la práctica, que debe traducirse en un programa informático. Sería difícil para los robots determinar, por ejemplo, si alguien está herido y fuera de combate o si los soldados están o no en proceso de rendirse*.

En definitiva, con las tecnologías en el campo de batalla aunamos el debate ético y el debate jurídico y se cuestiona por un lado, si deben ser las máquinas quiénes decidan quién debe morir y quién debe vivir en el campo de batalla y por otro lado, quien debe asumir la responsabilidad legal de dicha decisión.

Parece que sí las máquinas o los robots no tienen capacidad de discernimiento moral, si causan pérdidas de vida no se les puede exigir ningún tipo de responsabilidad, como sería normalmente el caso si las decisiones las hubieran tomado seres humanos.

Hay quien ha planteado si entonces la responsabilidad legal puede recaer, entre otros, en los programadores informáticos, los fabricantes o vendedores de equipo, los jefes militares, los subordinados que despliegan esos sistemas o los dirigentes políticos.

En todo caso no será fácil que cualquiera de todos ellos quisiera asumir una responsabilidad por una acción de tan magnas consecuencias y con tantos posibles responsables intervinientes.

Entre las propuestas que plantea el Relator Especial en su Informe para Naciones Unidas se proponen varias soluciones:

- *Dado que es posible exigir a un jefe responsabilidades por las acciones de un subordinado autónomo humano, puede parecer análogo exigírselas por las de un subordinado autónomo que sea un robot. Sin embargo, tradicionalmente solo incurren en responsabilidad de mando cuando los jefes sabían o debían haber sabido que el subordinado iba a cometer un delito y no tomaron medidas para impedirlo o no castigaron al infractor después del hecho.*

- *Indica que será importante establecer, entre otras cosas, si los jefes militares están en condiciones de comprender la compleja programación de los robots autónomos letales suficientemente bien para incurrir en responsabilidad penal.*

- *Se ha propuesto que al menos se exija responsabilidad por daños y perjuicios a los programadores y los fabricantes, empleando un esquema similar al de la responsabilidad civil por productos defectuosos. Sin embargo, la legislación relativa a la responsabilidad por los productos sigue siendo en gran parte inédita en los distintos países.*

- *También es cuestionable si es justo que sean las víctimas quienes tengan que iniciar acciones civiles por daños y perjuicios, ya que tendrían que incoar la acción en un país extranjero y a* menudo carecerían de los recursos necesarios.

El informe de Naciones Unidas finalmente propone varias soluciones para establecer la responsabilidad legal: *(i) imponerse al empleo de robots autónomos letales la atribución previa de responsabilidad; (ii) llevar a cabo un seguimiento y reconstrucción precisos de lo ocurrido durante la ejecución de operaciones letales, con la instalación de dispositivos de grabación y exámenes a posteriori de todo el material grabado; (iii) o un sistema de reparto de la responsabilidad entre varios candidatos posibles. Y en todo caso se argumenta la necesidad de modificar las normas relativas a la responsabilidad de mando para que abarquen también el empleo de robots autónomos letales.*

Hay quien en todo caso intenta buscar la forma de garantizar que las máquinas y funcionen bajo criterios éticos, fundamentalmente los robots, de manera que puedan llegar a pensar o razonar como un individuo. Algoritmos que, como un combatiente más, dispongan de razonamientos siguiendo criterios éticos en la toma de decisiones.

Pese a esta nueva realidad, no se debería descuidar al combatiente humano.

Al individuo cuyo entrenamiento pasa del "cuerpo a cuerpo" a "una pantalla"; del uso de las armas en el campo de batalla, a su dirección desde cientos o miles de kilómetros. ¿Estamos convirtiendo al soldado una máquina? ¿Cómo puede ejercer su capacidad de decidir en esta situación?.

No parece que el efecto psicológico provocado al combatiente en el campo de batalla por una amenaza, sea el mismo que el provocado frente a sistemas de toma de

decisiones automáticos o controlados desde una oficina por un ordenador. O quizás debamos entender que el nivel de amenaza percibido por el combatiente genera los mismos efectos, venga ésta de una fuerza letal física o de una ciberfuerza letal.

Ocurre en todo caso que, cuando el combatiente se enfrenta a una amenaza a cientos de kilómetros podría haber dudas en cuanto al grado de intencionalidad maliciosa que hay tras su sentimiento de amenaza y ello podría generar igualmente dudas al combatiente sobre los riesgos que debe asumir o las consecuencias de su actividad y/o inactividad.

Es posible que el deterioro del rendimiento físico del combatiente haya mejorado con las tecnologías (desde luego no es el mismo esfuerzo físico el realizado en el campo de batalla que frente a un ordenador) y que por tanto con ello, su capacidad de resistencia física también sea mayor; Pero quedaría por analizar si el trauma de la agresión interpersonal, el miedo y el horror en la corta distancia, han sido sustituidos por algún tipo de estrés o por el contrario estamos convirtiendo a los cibercombatientes en puras máquinas.

EN CONCLUSIÓN

Quién hace unos años podía imaginar la situación en que nos encontramos. La velocidad a la que se suceden las innovaciones tecnológicas y el fenómeno de la globalización han transformado profundamente la sociedad en todos sus sectores, sin distinción.

Estamos sin duda en un escenario de innovación disruptiva que a todas luces no parece haber llegado a su fin. Sector civil y sector militar deben ser más aliados que nunca frente a la lucha por la convivencia en paz en el Ciberespacio. Pero pese a la insistencia de las instituciones en que las normas “offline” nos sirven para la vida “online”, la realidad es que reglas morales y éticas que hasta regían las relaciones sociales entre los individuos y entre los Estados se están transformando, o ya lo han hecho. Consiguientemente algunas normas jurídicas ya no sirven al objeto de proporcionar una protección igual, justa y con seguridad jurídica.

Hay que trabajar por el cambio.

BIBLIOGRAFÍA

Pastor Ridruejo, José Antonio. 2008. Editorial Tecnos. Grupo Anaya S.A. Curso Internacional de Derecho Internacional Público y Organizaciones Internacionales.

Edgar, Timothy. Enero/Marzo 2015. La Vanguardia Ediciones. Revista Vanguardia Dossier nº 54. ¿Modifican las armas cibernéticas las leyes sobre la guerra?, págs. 26-31.

Presidente Prieto Osés, Ramón; Miembros Alejandro, Hernández Mosquera; Candón Adán, Alfonso; Murillo Tapia, Ana; Quesada Alcalá, Carmen; Enríquez González, Nicolás; Calderón Moreno, Joaquín. Abril 2013. XXXIII Curso de Defensa Nacional, Ciberseguridad nuevo reto del siglo XXI: Aspectos Organizativos. Grupo de Trabajo nº 3 del CESEDEN.

Reguera Sánchez, Jesús. 2015. Grupo de Estudios en Seguridad Internacional, GESI. "Aspectos legales en el ciberespacio. La ciberguerra y el Derecho Internacional Humanitario". Disponible en http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

Simón, Luis. Real Instituto Elcano, 2015. Offset Strategy: ¿hacia un nuevo paradigma de defensa en EEUU? http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/Elcano_es/Zonas_es/ARI14-2015-Simon-offset-strategy-hacia-un-nuevo-paradigma-de-defensa-en-EEUU

Heyns, Christof. 9 abril de 2013. Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo: Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias.

U.S. Department of Defense, "Defense Innovation Days" by Secretary of Defense Chuck Hagel, Newport, Rhode Island, Wednesday, September 03, 2014. http://www.defense.gov/speeches/speech.aspx?speechid=1877

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: La política y la gobernanza de internet - El papel de Europa en la configuración de la gobernanza de internet", 2015.

Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras Críticas

Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

Carta de las Naciones Unidas.

Comunicación de la Comisión Europea al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre "La creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos", 2001.

Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la "Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro", 2013.

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión, 2013.

Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la "Estrategia para una industria europea de la defensa más sólida y Competitiva", 2007.

Directiva 2009/81/CE del Parlamento Europeo y del Consejo de 13 de julio de 2009 sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE.

Ley 24/2011, de 1 de agosto, de contratos del sector público en los ámbitos de la defensa y de la seguridad.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior.

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-47_sp.pdf.

ALGUNAS CONCLUSIONES

Jordi Marsal Muntalà.
Adjunto civil al Director del CESEDEN

La evolución y las revoluciones tecnológicas siempre han tenido profundas consecuencias en el desarrollo de todos los aspectos de las sociedades y también en los aspectos militares y políticos relacionados con la seguridad y la defensa. Los procesos de innovación cada vez han aumentado sus ritmos, las tecnologías que podían tener incluso siglos de vigencia cada vez acortan su tiempo de vida significativo. En el siglo XX, especialmente en su segunda mitad tras el fin de la Segunda Guerra Mundial, el ritmo de cambios es frenético y lo que pueda suceder en el siglo XXI es casi imprevisible.

El factor tecnológico puede determinar la superioridad en el enfrentamiento y supone también un elemento de disuasión frente a quienes poseen un menor desarrollo tecnológico. Sin embargo por sí solo no es una garantía de éxito si no va acompañado por un personal entrenado adecuadamente para utilizar eficazmente estas tecnologías y por un desarrollo doctrinal y estratégico adecuado a las nuevas tecnologías.

Conseguir un suficiente desarrollo tecnológico que permita la superioridad requiere de unos recursos económicos sostenidos para la investigación y el desarrollo que permitan la innovación tecnológica.

La innovación es elemento fundamental para la superioridad tecnológica. Sin suficientes recursos económicos y humanos es difícil garantizar la innovación. Pero también es un peligro para la innovación la resistencia al cambio que acostumbran a tener las organizaciones, especialmente cuanto más complejas son. Toda innovación supone cambios tanto organizativos como funcionales que pueden generar reticencias. Estas reticencias pueden encontrarse tanto en las industrias de defensa como en la Fuerzas Armadas; por ello se requiere un fuerte liderazgo que impulse la innovación y permita superar estas reticencias. Así procesos de innovación tecnológica y procesos de transformación militar están íntimamente correlacionados.

No todas las innovaciones tecnológicas tienen las mismas consecuencias. Algunas suponen mejoras en las capacidades ya existentes. Otras pueden producir auténticas disrupciones que permiten un salto cualitativo que permite la auténtica superioridad en el enfrentamiento. Estas tecnologías disruptivas requieren una atención prioritaria si queremos mantener o recuperar la superioridad. En momentos de dificultades económicas se acostumbra a incrementar el interés por lo inmediato para solucionar las carencias presentes y pasan a ocupar un lugar más secundario las preocupaciones estratégicas a medio o largo plazo.

La innovación disruptiva tiene sus resultados a medio y largo plazo, por ello requiere de este liderazgo estratégico, político y militar, que sin olvidar las necesidades

inmediatas tenga una visión a largo plazo de cuáles serán los escenarios estratégicos, pero también operativos, que exigirán nuevas capacidades para dar respuesta a los retos que se planteen.

En este marco es necesario ir más allá de lo estrictamente tecnológico y analizar las consecuencias que se siguen de las disrupciones tecnológicas. Estas pueden, acostumbran a, producir disrupciones en los niveles doctrinales y también en los marcos legales. Por ello es necesario, para sacar el máximo resultado a las innovaciones disruptivas, analizar las consecuencias que van a tener sus aplicaciones en las capacidades y en el uso de los sistemas de armas. Será imprescindible introducir los cambios doctrinales para que la utilización de las nuevas capacidades sea adecuada a los nuevos escenarios que la propia innovación acostumbra a inducir.

Pero también será necesario analizar si los marcos legales y jurídicos existentes (desde las leyes internacionales y nacionales hasta las reglas de enfrentamiento) dan respuesta a nuevas situaciones que surgen con la aplicación práctica de las nuevas capacidades. Tampoco podremos dejar de lado las implicaciones éticas que ello suponga. Todo esto generará debates no solamente en el ámbito de la comunidad política y militar de la seguridad sino que también implicará el posicionamiento de distintos actores sociales y en diversos ámbitos (universitarios, periodísticos, religiosos, etc.). Así será necesario un elevado grado de sensatez para que no se produzcan disfunciones entre el debate teórico y las necesidades prácticas en unos conflictos cada vez más complejos e imprevisibles, donde lo regular y lo irregular, lo simétrico y lo asimétrico se mezclen en lo híbrido. Escenarios en que puede ser necesario aplicar al mismo tiempo normas vigentes tradicionalmente en el derecho humanitario y el derecho de guerra, junto con nuevas regulaciones para hacer frente a lo híbrido o poder combatir a aquellos que no respetan ninguna norma legal o ética.

Hemos visto y analizado algunos ejemplos históricos de la aparición de tecnologías disruptivas o la aplicación disruptiva de tecnologías existentes y sus consecuencias. Tras la guerra fría hemos asistido a disrupciones basadas en tecnologías de la comunicación aplicadas al mando y control o en tecnologías de precisión que han dado lugar al llamado armamento inteligente, que han coincidido con nuevos escenarios y nuevos actores no tradicionales; todo lo cual ha conducido a la necesidad de nuevas tipificaciones de los conflictos y a las misiones, tradicionales y nuevas, que deben realizar las fuerzas armadas.

De un mundo bipolar pasamos a un mundo unipolar que produjo una década, la de los noventa del siglo pasado, de un gran optimismo que para algunos suponía incluso el fin de la historia o un mundo en paz, con la consiguiente disminución de los presupuestos para la seguridad y la defensa. Pero después hemos visto que la realidad no era tan simple y que nuevos escenarios de riesgos y amenazas surgían en el horizonte y llegaban a las puertas de nuestras casas. Hoy no acabamos de saber si avanzamos hacia un mundo multipolar o apolar. Tal vez un mundo de retorno a escenarios más parecidos a lo medieval o a lo pre-westfaliano.

Los Estados Unidos, cuya cultura estratégica se basa en la preponderancia de lo tecnológico, actor central de la etapa unipolar, empieza a darse cuenta de que la superioridad tecnológica, basada en una serie de tecnologías disruptivas surgidas en la segunda mitad del siglo pasado, empieza a estar en cuestión. Otros actores, estatales pero también no estatales, tienen cada vez más acceso a estas tecnologías y la gran diferencia cualitativa existente podría perderse o convertirse solamente en una relativa superioridad cuantitativa.

Para evitar que esto pueda acontecer el Pentágono ha lanzado una nueva iniciativa de la cual forma parte la denominada "tercera estrategia offset" que pretende conseguir una nueva innovación tecnológica disruptiva dotada con importantes recursos financieros para los próximos años. Iniciativa en la que trabajarán coordinadamente la administración del Departamento de Defensa, industria de defensa y think tanks especializados. Si se consiguen los resultados esperados podemos asistir a una nueva revolución en asuntos militares y las consecuentes transformaciones organizativas, funcionales y doctrinales.

Esta situación podría aumentar de forma aún más radical el gap tecnológico entre ambas orillas del Atlántico, hasta tal punto que la interoperabilidad resultase totalmente imposible. Este hecho no sería deseable ni para los actores europeos ni el norteamericano. Así es necesaria la implicación de los países europeos, también en el marco de la OTAN, en este proceso de innovación. Esto requiere voluntad política y recursos financieros adecuados por parte de los países europeos y de la propia UE, así como amplitud de miras por parte de los EEUU.

De esta necesaria colaboración se pueden seguir consecuencias fundamentales para las capacidades militares futuras, para las bases tecnológicas e industriales para la seguridad y la defensa, para las futuras doctrinas y estrategias políticas y militares. Y España no puede ni debe estar al margen de este proceso.

Estamos hablando tanto de nuevas tecnologías que irán surgiendo durante los años de desarrollo de la iniciativa como de la profundización en tecnologías ya existentes peo que pueden desarrollarse aún más o en su aplicación de una forma distinta y disruptiva.

El área tecnológica central será la robótica, los sistemas no tripulados (UAV's) o remotamente tripulados (RPA's), tanto para el espacio aéreo como el terrestre y el marítimo. El espacio submarino recobra una gran importancia sobre todo en el marco de las estrategias A2/AD y que afectará tanto a los sensores como a submarinos con tecnología AIP.

Las tecnologías aplicables en el ciberespacio, tanto defensivas como ofensivas, con especial consideración para el Big Data, jugarán un gran papel para garantizar la seguridad tanto estratégica como táctica en el campo de batalla.

También serán centrales las tecnologías para armas de energía dirigida y armas láser, con específica incidencia en la defensa antimisiles.

Seguirán profundizándose las tecnologías relacionadas con los ataques de precisión y las relacionadas con nuevos materiales, con especial interés en las nanotecnologías, por ejemplo en el campo del grafeno.

Se pasará de las estrategias Air-Land Battle a las de Air-Sea Battle y en un marco en que la proyección tradicional de fuerzas se irá sustituyendo por los ataques de profundidad y conducidos a distancia, con su incidencia en los sistemas de mando y control y las tecnologías relacionadas con la aeronáutica para este tipo de ataques o de control global.

Evidentemente estos desarrollos tecnológicos serán realizados en EEUU de acuerdo con su papel como gran actor global que quiere mantener su hegemonía, al menos en el campo militar. Por ello para la UE o sus países como España no se tratará de una traslación mecánica sino adecuada a la clase de actor que quieran y puedan ser. Así no todas las tecnologías tendrán el mismo interés ni la misma prioridad; será necesario priorizar en función de intereses estratégicos e industriales y también del nivel económico que estemos dispuestos a asumir.

La Dirección General de Armamento y Material (DGAM) del Ministerio de Defensa desde hace ya muchos años concede especial importancia a los procesos de innovación tecnológica y se doto de un instrumento, el Observatorio Tecnológico, para estar al día de la evolución de la investigación y desarrollo de nuevas tecnologías y con especial interés en aquellas tecnologías que pudiesen tener efectos disruptivos de interés para nuestras capacidades. Este es un marco y unas actividades que debemos potenciar al máximo posible con recursos humanos, materiales y económicos especialmente en un proceso de concentración de los procesos de adquisición y puesta en marcha de nuevos programas de inversión.

Estas inversiones deben tener en cuenta la adquisición de sistemas de armas necesarios, en muchos casos con una necesidad inmediata, y también la adquisición de tecnologías que nos permitan planificar a largo plazo.

Es prudente y necesario adquirir aquellos sistemas que responden a requerimientos urgentes condicionados por los escenarios presentes y por las misiones más probables a corto y medio plazo. Sin embargo si nos quedamos en ello podemos quedarnos a años luz del desarrollo tecnológico internacional y especialmente de nuestros aliados con los que debemos operar y no estar preparados para posibles escenarios a largo plazo. Tener capacidades tecnológicas, personal con adecuado know how, e industrias punteras en determinadas tecnologías es una condición necesaria y una garantía para poder adaptarse a las amenazas y a los escenarios que surjan en períodos útiles para darles respuesta con un uso innovador de capacidades existentes o la adquisición de nuevas capacidades.

Cada ciclo inversor debe tener en cuenta estos distintos factores y destinar unos recursos adecuados, en función de ambiciones y posibilidades, sobre todo para la definición y adquisición de tecnologías. Como los recursos siempre son limitados es necesaria una planificación que defina prioridades, y estas especialmente deben dirigirse a la adquisición y dominio de la tecnologías disruptivas que permitan nuestra superioridad en el enfrentamiento en los escenarios posibles a medio y largo plazo, y que asigne correctamente los recursos.

Es necesario un planeamiento realista que permita un Plan Director de I+D+i con unos recursos financieros a medio y largo plazo para garantizar la continuidad que dé sus frutos para el planeamiento de capacidades a medio y largo plazo.

España tanto a través de su pertenencia a la OTAN y a la UE y por sus relaciones bilaterales debe seguir todo el proceso de innovación iniciado y conseguir participar en los resultados de aquellas tecnologías disruptivas más útiles para nuestro planeamiento, lo que puede tener su expresión en el Convenio de Defensa con EEUU.

Nuestro país por su situación geopolítica y por tradición tiene una presencia naval tanto en sus propias aguas territoriales como en otras zonas marítimas para garantizar la libertad y la seguridad de tránsito para productos básicos para nuestra economía y desarrollo (desde las capturas pesqueras al tránsito de productos energéticos). Por ello las tecnologías relacionadas con nuestra acción naval pueden ser de gran interés (desde sensores submarinos a tecnología AIP).

Dada nuestra colaboración con el sistema de defensa antimisiles aquellas tecnologías relacionadas con estos sistemas que puedan significar cambios incluso geoestratégicos también pueden ser de nuestro interés.

Debemos definir cuál pueda ser nuestro interés y nuestras posibilidades con las tecnologías de energía dirigida y láseres (de ello hemos tratado en este cuaderno) por sus consecuencias tanto en los sistemas de armas como en las capacidades industriales propias.

El campo de la automatización, la robótica y los artefactos dirigidos remotamente serán fundamentales en los futuros escenarios y en las estrategias para darles respuesta. Las consecuencias de la aplicación de tales tecnologías van más allá de lo tecnológico e industrial ya que tendrán consecuencias en la planificación de las necesidades y características de personal, en la organización y funcionamiento de las unidades, y en importantes cambios doctrinales.

No podemos tampoco olvidar el campo de las tecnologías en el ciberespacio, tanto de uso defensivo como ofensivo, básicas tanto para la conciencia situacional de las unidades como en la defensa de infraestructuras y otros intereses económicos, sociales o militares para conseguir una plena operatividad y eficacia del Mando Conjunto de Ciberdefensa, por ejemplo.

Sistemas de mando y control, armas de precisión, furtividad de los sistemas de armas, utilización de nuevos materiales con especial incidencia de los relacionados con la nanotecnología (el grafeno cada vez cobrará mayor importancia y en su desarrollo y producción tenemos capacidades significativas tal como hemos visto), son también campos tecnológicos en los que debemos estar presentes.

A todos ellos debemos sumar también los aspectos relacionados con los cambios doctrinales que la aplicación de tales tecnologías van a significar. Desde el papel del uso ofensivo del ciberespacio a las acciones dirigidas desde la distancia o a las posibilidades de despliegue y mantenimiento de los individuos y las unidades por la aplicación de nuevas tecnologías relacionadas con el almacenamiento de energía deberemos trabajar en profundos cambios doctrinales, coherentes con los que se produzcan en nuestros aliados o en las organizaciones internacionales de las que formamos parte. El Mando de Transformación de la OTAN deberá jugar un papel central en este proceso al cual debemos contribuir, con sus consecuencias también en el campo de la formación tanto teórica como práctica.

Y también deberemos profundizar en la posibilidad o necesidad de cambios, adecuaciones o interpretaciones de distintos aspectos legales que inciden en la aplicación y uso de estas tecnologías disruptivas. Cuestiones como el uso de los RPA's armados con misiles para atacar objetivos delimitados con los menores daños colaterales (que igualmente pueden producirse); la atribución de ataques en el ciberespacio para poder responder contra un atacante identificado sin dudas o con dudas y definir una respuesta en el propio ciberespacio o contra objetivos materiales; los límites de autonomía de la que se puede dotar a los robots para actuar independientemente en el campo de batalla; cuestiones éticas relacionadas con el uso de nuevos materiales o de técnicas biomédicas y otras muchas cuestiones, deben ser debatidas profundamente para llegar a consensos que permitan la adecuación de los códigos legales y su aplicación, sin olvidar las posibles incidencias en las reglas de enfrentamiento que hemos ido definiendo a lo largo de los últimos veinticinco años. Estas cuestiones legales y éticas deben trasladarse también al campo de la formación de nuestro personal militar.

Estas son algunas de las conclusiones que pueden formularse como resultado de los trabajos individuales de cada capítulo y de las largas conversaciones y reflexiones colectivas que hemos tenido los autores de este cuaderno. Ya que aunque el trabajo concreto se ha centrado más en aquellas áreas y aspectos que hemos señalado en la introducción, esto nos ha permitido avanzar más en las reflexiones generales que permiten esta serie de conclusiones y recomendaciones que acabamos de exponer y que esperamos puedan ser de utilidad para los responsables de definir actuaciones y prioridades en lo tecnológico, lo doctrinal y lo legal.