La cuarta revolución industrial, el "algoritmo de guerra" y su posible aplicación a la Defensa española

Enrique Fojón | Infante de Marina y miembro del Grupo de Trabajo sobre Tendencias de Seguridad y Defensa del Real Instituto Elcano

Tema

De los retos actuales en el ámbito de la Defensa, muy probablemente el más importante es cómo adaptarla a los cambios que conlleva la cuarta revolución industrial. El Departamento de Defensa de EEUU ha comenzado a explorar las aplicaciones de la inteligencia artificial mediante el Proyecto Maven y el *algorithmic warfare*, que podrían servir de referencia para la innovación de la Defensa en España.

Resumen

Estamos asistiendo a un cambio de época profundo y sistémico en lo que se viene conociendo como la 4ª Revolución Industrial. Este cambio presenta ventajas y problemas de naturaleza disruptiva para la Defensa en los ámbitos tecnológicos, doctrinales, operativos, de personal y éticos, entre otros. El Departamento de Defensa de EEUU está desarrollando un nuevo concepto, el "algoritmo de guerra", para multiplicar las opciones y las decisiones que se obtienen algorítmicamente para obtener la superioridad tecnológica en el combate y afrontar los problemas derivados del empleo de los sistemas de armas autónomos (AWS en sus siglas inglesas). También ha puesto en marcha el "Proyecto Maven" para aplicar la inteligencia artificial (AI en las mismas siglas) a la inteligencia militar. Estas iniciativas se analizan en el contexto de la revolución tecnológica para explorar sus posibles aplicaciones al caso español.

Análisis

Klaus Schwab, presidente del Foro Económico Global (Davos), argumenta en su libro *La cuarta revolución industrial* [1] que ésta ha generado un cambio comparable al producido en su momento por la aparición del vapor, la electricidad y la computación. Una trascendencia que no se ha estudiado suficientemente para su aplicación a la guerra y los conflictos, a pesar del impacto de las nuevas tecnologías y su acceso a ellas por actores no estatales.

A primera vista, podría parecer extraño que en un foro como el de Davos se tratasen temas de seguridad, pero la Historia equipara las revoluciones industriales a las formas en las que se desarrollan las guerras. En 2016 elaboró un informe sobre "10 Trends for

[1] Klaus Schwab (2016), *The Fourth Industrial Revolution*, World Economic Forum.

(cont.)

the Future of Warfare"[2] con el que pretende analizar el impacto de la 4ª revolución industrial sobre la seguridad internacional en el futuro. Aquella difumina la separación entre paz y guerra, lo civil y lo militar, lo interior y lo exterior, lo público y lo privado y lo físico y digital. Estas revoluciones "son periodos de cambio discontinuo que convierten en obsoletos o subordinados los medios existentes para conducir la guerra".[3] Además, permiten a actores no estatales el acceso a tecnologías de uso militar que, mediante la llamada "democratización de la destrucción", les proporciona capacidades necesarias para causar daños, ganar apoyos o minar la moral de los oponentes.

Las barreras tecnológicas entre las civiles y militares están desapareciendo. El anterior secretario de Defensa estadounidense, Ashton Carter, reveló que la *Third Offset Strategy*, una estrategia tecnológica para compensar los avances obtenidos por los adversarios de EEUU, partía del reconocimiento de que las capacidades de innovación del sector privado aventajaban a las militares y de que una relación más abierta con empresarios, academia e instituciones científicas sería vital para mantener la preeminencia de las capacidades militares estadounidenses. A medida que la tecnología militar evoluciona hacia una mayor automatización, concretamente hacia el desarrollo y perfeccionamiento de armas de control remoto, se pone en cuestión la necesidad de que sean las personas las que adopten determinadas decisiones. Todo ello ha dado lugar a controversias en cuanto al empleo de los mencionados sistemas AWS, especialmente sobre los letales (*lethal systems autonomous weapons*, LAWS,) también conocidos como robots criminales.

Tal y como se ha expresado en el marco del Convenio sobre Prohibición o Restricciones en el empleo de Ciertas Armas Convencionales, la creciente interacción entre sensores, algoritmos y municiones genera cuestiones legales, éticas, operativas y diplomáticas sobre la aceptabilidad de la autonomía en determinadas funciones críticas, particularmente sobre la selección de empleo o la identificación y aplicación de la capacidad de destrucción sobre blancos.[4]

Algoritmo de guerra

El Pentágono y el anterior subsecretario de Defensa, Robert O. Work, apoyaron el concepto del algoritmo de guerra a partir de abril de 2015. No pretendían crear una ecuación que pudiese resolver una guerra, pero reconocieron la importancia de incluir las matemáticas en el proceso de decisiones a todos los niveles. Al menos otros 30 países, incluyendo a China, Rusia, Irán e Israel, están desarrollando también armamento autónomo y la comunidad internacional necesita regular su desarrollo parar prevenir los riesgos que los algoritmos y la capacidad de autoaprendizaje de las máquinas traerán a los campos de batalla.

[2] https://www.weforum.org/agenda/2016/11/the-4th-industrial-revolution-and-international-security/.

[3] Michael G. Vickers y Robert C. Martinage (2004), *The Revolution in War*, Center for Strategic and Budgetary Assessments, Washington DC, diciembre, pp. 2-3.

[4] Heather Roff y Richard Moyes (2016), "Meaningful Human Control, Artificial Intelligence and Autonomous Weapons', *briefing paper* para el *Informal Meeting of Experts on Lethal Autonomous Weapons Systems, UN Convention on Certain Conventional Weapons*, abril, http://www.article36.org/wpcontent/uploads/2016/04/MHC-AI-and-AWS-FINAL.pdf.

Los algoritmos de guerra plantean el dilema vital de si se puede o debe regular, e incluso prohibir, ciertas tecnologías que, progresivamente, se conciben como sustitutos del juicio humano que se emplea en la guerra. Su utilización, especialmente la de algoritmos de autoaprendizaje, pone en cuestión alguno de los conceptos legales y de responsabilidad sobre los que se fundamenta la regulación de los conflictos armados, además de correr el riesgo de que se acabe perdiendo su control mediante el *hackeo*. Siendo el futuro desarrollo de los AWS un objeto de debate público, algunos se inclinan a un gradual desarrollo de códigos de conducta éticos sobre su uso, basado en principios consuetudinarios sobre los usos de la guerra, mientras que otros promueven su prohibición. Ese debate, que afecta al control democrático de las fuerzas armadas, no preocupa a algunos actores estatales y no estatales que desplegarían esos mismos sistemas sin reparos éticos o jurídicos. Por el contrario, las fuerzas armadas se enfrentan a consideraciones éticas y de control democrático para aplicar tecnologías como las de análisis y explotación de datos masivos (*big data*), el autoaprendizaje de las máquinas (*machine learning*) o la interlocución con las máquinas (*chatbots*).

El debate sobre el algoritmo de guerra es algo más que discutir un término legal o técnico porque el concepto enmarca nuevas tecnologías que deben estudiarse para considerar su regulación. Imaginemos su aplicación en un contexto donde un misil se dirige hacia un vehículo de combate poniendo en riesgo a la tripulación. A pesar de lo excelente que pueda ser su adiestramiento, la situación altera su capacidad de análisis y reacción. En esos momentos, la toma de decisiones podría confiarse a la AI para salvar las vidas de la tripulación sin su intervención. Sería lo que los investigadores de la Facultad de Derecho de Harvard denominan "algoritmo de guerra" en su Programa sobre Derecho Internacional y Conflicto Armado, algo así como la AI cuando opera en el contexto del combate. No sería exclusivamente un término legal o técnico sino un concepto útil para analizar nuevas formas de tecnología que deben estudiarse para su regulación.[5]

El empleo de algoritmos en la vida diaria es algo habitual. Un algoritmo no es más que secuencia de pasos lógicos para resolver un problema y se aplica tanto por los ordenadores como por cualquiera de los dispositivos informáticos de uso cotidiano.[6] Un algoritmo de guerra se compone de un código de computación y de una plataforma mediante la que se combinan información y decisión sin intervención humana para poder operar en un contexto bélico. No tiene por qué aplicarse sólo en situaciones de combate para ayudar a identificar, discriminar, localizar y atacar un blanco, sino también en cometidos como proporcionar apoyo médico o logístico, entre otros. Tampoco tienen por qué aplicarse exclusivamente a los sistemas autónomos, ya que existen algoritmos subyacentes que penetran a través de todos los sistemas, y deben identificarse como autónomos o no, según el programa de Harvard mencionado anteriormente.

[5] Dustin A. Lewis, Gabriella Blum y Naz K. Modirzadeh (2016), *War-Algorithm Accountability*, Harvard Law School Program on International Law and Armed Conflict, agosto, https://lawfareblog.com/accountability-algorithmic-autonomy-war.

[6] Brian Christian y Tom Griffiths (2016), *Algorithms to Live By. The Computer Science of Human Decisions*, Henry Holt & Co.

(cont.)

El Departamento de Defensa de EEUU define un AWS como un sistema de armas que, una vez activado, puede seleccionar y batir blancos sin necesidad de que actúe el operador humano. Incluye los sistemas supervisados por operadores que pueden cancelar la operación. Básicamente es un arma que puede emplearse en cualquier dominio –tierra, mar, aire, espacio y ciberespacio, o combinaciones de ellos– y se considera que abarca significativamente más que la plataforma que dispara la munición. Los AWS ocupan ese extraño espacio entre las armas y los combatientes[7] y pueden ser autónomos, si tienen capacidad para cumplir sus cometidos escogiendo con independencia entre las diferentes opciones posibles en función de su conocimiento del mundo, de sí mismo y de la situación, o automáticos, o si se limitan a tomar decisiones y acciones sin que puedan salirse de las condiciones preestablecidas.

El Proyecto Maven

En abril de 2017, el entonces subsecretario de Defensa, Bob Work, creó el *Algorithmic Warfare Cross-Functional Team*, también conocido como Proyecto Maven. El Departamento hace tiempo que financia proyectos de I+D+i en inteligencia artificial y ya ha puesto en servicio sistemas semiautónomos, pero el Proyecto Maven es el primero que pretende incorporar sistemas de autoprendizaje y redes neuronales en sus últimas versiones comerciales a la inteligencia militar. Es un proyecto estrella del Pentágono que financia tecnologías de inteligencia artificial, especialmente las que sean de autoaprendizaje (*machine learning*), y que puedan desplegarse en un teatro de operaciones seis meses después de recibir la financiación.

El equipo del Proyecto Maven cuenta con el apoyo de la Unidad Experimental de Innovación de la Defensa (*Defense Innovation Experimental Unit*, DIUx), una Unidad creada por el anterior secretario de Defensa, Ashton Carter, que sirve como un centro de atracción de la innovación del sector privado para resolver problemas tecnológicos militares. Ubicada en Silicon Valley, California, trata de cambiar la cultura burocrática del Pentágono asociándola a la cultura de innovación de las empresas y centros tecnológicos allí instalados.

Antes de su adopción, el Departamento fue asesorado por expertos en inteligencia artificial de la industria y de la academia para buscar una solución al problema de procesar gran número de datos con vidas humanas en juego y con el peligro de que los fallos ocasionales llevaran al desastre. El asesoramiento incluyó también la estructuración de los proyectos de adquisición, testado y desarrollo de la inteligencia artificial porque el Departamento estaba habituado a un proceso distinto, con muchos años de duración y muchas organizaciones participando en el proceso de forma secuencial. En la era digital el sistema quedó obsoleto y el proyecto Maven ha implantado un enfoque diferente, modelado según técnicas de gestión de proyectos del sector tecnológico comercial: prototipos y la infraestructura subyacente se desarrollan iterativamente y se comprueban por los usuarios sobre la marcha. Los proyectistas pueden adaptar sus soluciones a las necesidades del usuario final y estos pueden

[7] Rebeca Crootof (2016), "War torts: accountability for autonomous weapons", *University of Pennsylvania Law Review,* vol. 164, nº 6, mayo.

preparar sus organizaciones para hacer un empleo rápido y eficaz de la inteligencia artificial.

El Departamento de Defensa cree haber hallado en la AI y en los AWS nuevas fuentes de ventaja militar. Unos ámbitos liderados por las empresas y universidades estadounidenses y que hasta ahora no había sabido aprovechar la tecnología militar. Por eso el Proyecto Maven pretende desarrollar *softwares* que sean capaces de absorber más cantidad de información y de más fuentes sin participación humana o con limitaciones programadas si es posible, especialmente en los campos de ciberdefensa y misiles; y, si no lo es, poder asesorar a los operadores humanos sobre como emplear mejor la inteligencia artificial.

Implicaciones para la Defensa española

La referencia en este ARI a las iniciativas del Departamento de Defensa de EEUU es circunstancial, porque sólo se trata de mostrar una forma, entre las posibles, de encontrar una solución a un problema. La 4ª revolución industrial plantea a las fuerzas armadas de todos los países, incluido España, el problema de adecuar sus instrumentos militares a ella si quieren operar con prontitud y eficacia. Para ello deben apoyarse en la búsqueda de partenariados como el alcanzado el 19 de enero de 2018 entre Francia y el Reino Unido, aprovechando la visita del presidente Enmanuel Macron a Londres, para reunir sus capacidades industriales y académicas al servicio de la inteligencia y de la ciberseguridad en apoyo de sus fuerzas armadas.

Las Fuerzas Armadas españolas disponen de las plataformas, vehículos, buques y aeronaves para obtener y operar una Fuerza Conjunta en un ámbito multidominio, pero necesitan de los sensores que permitan la percepción del campo de batalla con la necesaria rapidez para tomar las oportunas y correctas decisiones. No dotar a las plataformas de los nuevos sistemas de AI (*intelligence payload systems*) las condena a la obsolescencia.

El primer paso es tomar conciencia de la necesidad, y aunque se conoce que la tecnología y la innovación son los fundamentos de la 4ª revolución industrial, hay que contar con la resistencia a la adaptación. En un ambiente de enormes burocracias administrativas, tanto públicas como privadas, los cambios son difíciles, y la colisión entre nuevas tecnologías y anteriores estructuras y sistemas de trabajo, tienen efectos imprevisibles.

Aprovechando la experiencia estadounidense, se podrían tomar en cuenta las conclusiones del Consejo Asesor de Innovación de la Defensa del Departamento de Defensa que sostiene que el Departamento no tiene un problema de innovación, sino de gestión de la innovación.[8] Entre otras, el Consejo recomienda diseñar una trayectoria ágil para identificar y priorizar los problemas operacionales más acuciantes, así como constituir equipos multidisciplinares que diseñen modelos orgánicos y disciplinas para

[8] Un extracto de las conclusiones del *Defense Innovation Advisory Board* se puede consultar en http://www.defenseone.com/technology/2018/01/heres-how-stop-squelching-new-ideas-eric-schmidts-advisory-board-tells-dod/145240/.

alcanzar rápidas soluciones. Propone implantar incubadoras para apoyar a las empresas innovadoras (*startups*) en tecnologías aplicables al ámbito militar, proporcionándoles financiación, instalaciones y asesoramiento. Así mismo, propone crear una carrera militar en innovación, ciencia y tecnología, al igual que ya han hecho algunas fuerzas armadas con la ciberdefensa, y fomentar la familiarización y educación de los altos cargos del Departamento en estas materias para que puedan reconocer, apreciar y apoyar las ideas emprendedoras, los subordinados de talento y la innovación exitosa en el sector privado.

Al igual que la nueva *National Defense Strategy* de EEUU incluye ya alguna de las reformas orgánicas y administrativas sugeridas por su Consejo Asesor, las próximas Directivas de Defensa Nacional deberían incluir algunas directrices para impulsar la transformación tecnológica. Pero además de cambios de mentalidad y de organización, la inversión presupuestaria de la Defensa española tiene que tener en cuenta la prioridad de la innovación para adecuar sus partidas de I+D+i para fomentar y sostener el avance tecnológico de sus fuerzas armadas. Para ello podría ser interesante crear un Consejo Asesor de Innovación de la Defensa (CAID) con representantes de la industria, academia, administración y las fuerzas armadas como órgano asesor del ministro de Defensa en la conducción de la innovación tecnológica.

Conclusiones

Cuando se alude a los algoritmos de guerra se hace referencia a ecuaciones matemáticas diseñadas para dar a las fuerzas armadas un mayor conocimiento de lo que ocurre en el campo de batalla, auxiliando a su personal a reaccionar antes que los adversarios y así alcanzar victorias o, mejor aún, disuadir al enemigo del enfrentamiento. Los rápidos avances en inteligencia artificial y los sistemas de armas autónomos o automáticos introducirán nuevas técnicas de combate en las que se acentúe la colaboración entre personas, máquinas y equipos de combate. Esas nuevas aplicaciones serán los impulsores primarios de una emergente revolución técnico-militar.

El Proyecto Maven recurre al milagro de la tecnología y a la capacidad de los humanos de hacer más con menos, incrementando las capacidades militares a un mayor nivel. No se deciden las capacidades militares necesarias eligiendo entre un catálogo cósmico de opciones ni renovando todo lo que ya hay. Por el contrario, hay que apostar por los avances tecnológicos que más determinen las formas de combatir en el futuro. No hay fórmulas predeterminadas para el éxito, pero hay que probar con factores como el liderazgo, el compromiso y la capacidad que proporciona el talento.

Por eso, la aportación del Proyecto Maven o del *war algorithm* no se reducen a la mera tecnología, sino a la búsqueda de talento, al ensayo de nuevos procedimientos operativos, a la adaptación del proceso presupuestario, la transformación orgánica o la colaboración cívico-militar para captar el talento y el liderazgo necesario que precisan las fuerzas armadas para hacer frente a las lentas reacciones de sus grandes burocracias y potenciar la industria. Se puede seguir el camino abierto por EEUU o por otros países, pero España no puede eludir el reto que supone adaptar su Defensa a la 4ª revolución industrial y contar con sus propios algoritmos de guerra.