

# Componentes tecnológicos de la nueva militarización

PERE BRUNET

A pesar de los esfuerzos de Naciones Unidas y de múltiples organizaciones en todo el mundo, a pesar de la evidencia reiterada de los múltiples fracasos humanitarios que han ido acumulando las operaciones militares –Vietnam, Afganistán, Irak, Libia, etc.–, a pesar de que los grandes retos que deberá afrontar la humanidad este siglo son globales y planetarios, los Estados-nación continúan pensando en falsas soluciones basadas en teorías de seguridad nacional militarizada, y continúan incrementando sus presupuestos militares. Lejos de entender que la construcción mundial de la paz, la seguridad humana y las necesarias políticas de cuidado de las personas requieren una reducción significativa de los presupuestos militares, los Estados se plantean nuevas políticas de defensa que curiosamente incluyen partidas para el desarrollo o compra de sistemas de ataque. Europa, sin ir más lejos, ha acordado poner en marcha el Fondo Europeo de Defensa (EDF) junto con los programas preparatorios PADR y EDIDP, como instrumento de la UE para apoyar la investigación y el desarrollo de nuevas armas y tecnologías militares en el período 2021-2027.<sup>1</sup>

En todo caso, los nuevos avances tecnológicos tienen obviamente una repercusión en los sistemas militares avanzados, y ello puede cambiar radicalmente los escenarios de los conflictos armados en los próximos años.<sup>2</sup> En lo que sigue, nos concretaremos, en aras de la brevedad, en algunos aspectos que consideramos relevantes. Revisaremos y analizaremos la militarización del ciberespacio, hablaremos de los ataques a distancia, estudiaremos lo que nos pueden deparar los sistemas no tripulados y la inteligencia artificial y comentaremos asimismo los com-

<sup>1</sup> El EDF cuenta con un presupuesto de 8.000 millones de euros en el marco financiero plurianual actual (2021-2027), el presupuesto de siete años de la UE. Se espera que los estados miembros agreguen miles de millones de euros de cofinanciamiento. Disponible en:

[https://ec.europa.eu/defence-industry-space/eu-defence-fund-edf\\_en](https://ec.europa.eu/defence-industry-space/eu-defence-fund-edf_en)

<sup>2</sup> Carol Turner (2018), «New technology and war: a view from the dark side», *Future Wars Conference on the Impact of New Technologies*, CND, Londres, noviembre de 2018. Disponible en: <https://morningstaronline.co.uk/article/new-technology-and-war-view-dark-side> El Programa está disponible en: <https://cnduk.org/wp/wp-content/uploads/2018/10/Future-Wars-Conference-Agenda.pdf>

ponentes tecnológicos de doble uso, con algunas conclusiones sobre esta escalada tecnológica militar.

## El ciberespacio y la ciberguerra

En los conflictos modernos los modelos de combate se están diversificando y ampliando de tal manera que las actuaciones de combate tradicional se complementan con medidas políticas, económicas, de información, de ataques informáticos, publicitarias e incluso de interferencia electoral.<sup>3</sup>

Estas actuaciones combinadas pueden tomar la forma de ciberataques, manipulaciones en las redes sociales, sistemas de presión económica con el fin de desestabilizar la opinión pública del adversario, llegando incluso a actuaciones coordinadas con la ciberdelincuencia, con el crimen organizado o con movimientos subversivos y terroristas.

**En los conflictos modernos los modelos de combate se diversifican con medidas políticas, económicas, de información, de ataques informáticos, publicitarias e incluso de interferencia electoral**

Sabemos de todo ello por personas como Edward Snowden, que en 2014 filtró a la prensa documentos que desvelaban un complejo entramado de agencias de inteligencia en numerosos países occidentales que habían establecido un sistema de vigilancia global y que recopilaban datos, documentos y comunicaciones de todo tipo con programas secretos de vigilancia masiva que rompían la seguridad de los sistemas operativos.

Muchos Estados están desarrollando capacidades de ciberguerra dentro de sus estrategias de defensa y seguridad, tanto ofensivas como defensivas. El concepto de ciberarma no existe desde un punto de vista jurídico, pero sí podemos decir que las armas cibernéticas no son objetos físicos, sino que deben estudiarse como elementos funcionales que realizan acciones con determinadas finalidades preestablecidas.

<sup>3</sup> Pere Brunet, Tica Font, Xavi Mojal y Joaquín Rodríguez , *Nuevas armas contra la ética y las personas. Drones armados y drones autónomos*, Centro Delàs, Informe 39, 2019, pp.12-13. Disponible en: [https://arxiu.centredelas.org/images/INFORMES\\_i\\_altres\\_PDF/informe39\\_DronesArmados\\_CAST\\_web\\_DEF.pdf](https://arxiu.centredelas.org/images/INFORMES_i_altres_PDF/informe39_DronesArmados_CAST_web_DEF.pdf)

Los ciberataques incluyen:

- El espionaje, como el que sufrió la cancillera Angela Merkel en 2014 por parte de la agencia NSA de los Estados Unidos, las grabaciones (hechas por la misma NSA) de conversaciones en la Bahamas, Kenia, Filipinas, México o Afganistán<sup>4</sup> o las del sistema Israelí Pegasus de la empresa NSO, que aprovecha vulnerabilidades para infiltrarse en los teléfonos móviles.
- Los ataques cibernéticos por sorpresa, que pueden ser de diversos tipos. Los DoS o de negación de servicios (*denial of services*) suelen bloquear un determinado servicio mediante la estrategia de saturar repentinamente el servidor informático con millones de peticiones simultáneas enviadas desde muchísimos puntos del planeta. Los troyanos son programas y aplicaciones aparentemente inofensivos que pueden llegar como adjuntos en correos electrónicos, que se instalan en los ordenadores y que pueden luego realizar acciones de espionaje, de bloqueo, modificación y borrado de datos, o incluso de detención del ordenador o de la red local. Otros ataques cibernéticos incluyen los sistemas de secuestro de datos (*Ransomware*) se introducen en los ordenadores de manera parecida a los troyanos para, tras un tiempo de reposo o hibernación, encriptar y bloquear el acceso a la información, que únicamente podrá recuperarse tras pagar un rescate, o bien los sistemas de tipo *Keylogger* que registran las pulsaciones del teclado para capturar contraseñas.
- El sabotaje a sistemas militares de comunicación, pero también a infraestructuras civiles de energía, agua, combustibles, transporte y comunicaciones. Estas acciones de sabotaje se realizan mediante ataques cibernéticos como los ya mencionados a los sistemas informáticos de control de las instalaciones objetivo.
- Ataques a los sistemas económicos de determinadas empresas y grandes organizaciones, como el que sufrió en 2017 el sistema nacional de salud del Reino Unido.
- La propaganda, la desinformación y la influencia en la opinión pública a través de las redes sociales, utilizando identidades inexistentes y transmitiendo mensajes tendenciosos. La empresa Cambridge Analytica utilizó el perfil psicológico de 220 millones de ciudadanos de los Estados Unidos para mandarles mensajes personalizados, además de influir en más de 200 procesos electorales en todo el mundo.

<sup>4</sup> Zach Schonfeld, «The Intercept Wouldn't Reveal a Country the U.S. Is Spying On, So WikiLeaks Did Instead», *Newsweek*, 23 de mayo de 2014. Disponible en: <http://www.newsweek.com/intercept-wouldnt-reveal-country-us-spying-so-wikileaks-did-instead-252320>

Una característica común a todos estos métodos de ciberataque es su inmaterialidad. Todos ellos se realizan usando los recursos existentes en internet y con herramientas de *software* que en muchos casos tienen una complejidad no excesiva. En muchos casos, además, aunque las infraestructuras objetivo estén dotadas de grandes medidas de seguridad, los sistemas ciberatacantes detectan y aprovechan aquellos errores humanos que de vez en cuando se producen y que generan rendijas que abren temporalmente la puerta a los atacantes.

La ciberguerra y los ciberataques son económicos, pueden ser muy destructivos, y han llegado para quedarse.

## Los sistemas militares no tripulados

Debemos distinguir entre los sistemas militares robóticos que pueden actuar sin intervención humana y los sistemas no tripulados. En el primer caso tenemos las

**Una característica común a los métodos de ciberataque es su inmaterialidad: todos ellos se realizan usando los recursos existentes en internet**

armas centinela desplegadas en muchas fronteras (que detectan movimientos de personas y pueden llegar a disparar, de manera supervisada o no), o los sistemas de defensa aérea y de protección activa de blindados y otros, que detectan amenazas mediante sensores y reaccionan de forma automática disparando contra posibles misiles y cohetes agresores en situaciones en las que la velocidad

de respuesta requerida es superior a la que podrían dar los humanos. Los sistemas militares no tripulados, en cambio, son equipos versátiles que, sin ser pilotados directamente por personas, pueden realizar funciones parecidas a las de los sistemas móviles tradicionales de combate. En este sentido, pueden mencionarse sistemas terrestres (carros de combate no tripulados), sistemas marítimos que han surgido básicamente como evolución de los submarinos y torpedos, y sistemas aéreos. Estos últimos son los denominados drones (UAV, *Unmanned Aerial Vehicles* en inglés) a los que nos referiremos en el resto de este apartado.

Un dron es un robot volador. Como vehículo aéreo, incluye todos los componentes tecnológicos necesarios para el vuelo y su control: sistema de propulsión, almacenamiento de energía, sistemas de posicionamiento (GPS o similares) y sistemas de control de vuelo para su estabilización y pilotaje automático hacia el destino

que se haya programado, además de para el despegue, aterrizaje y retorno a la base. Todos ellos son elementos de doble uso que encontramos tanto en los drones civiles de rescate, detección de incendios u otras emergencias como en los drones de uso militar. En tanto que robot, todo dron incluye además un cierto número de sensores junto con los componentes de comunicación con la base y los actuadores apropiados en base a su función. Los sensores suelen incluir cámaras para la obtención de fotos y vídeos que el sistema de comunicación transmite de forma segura y encriptada a los operadores en la base. Estos últimos elementos (sensores, cámaras y comunicación con los operadores en tierra) son también de doble uso tanto para operaciones civiles como para uso militar.

Los drones militares pueden tener funciones de reconocimiento o de ataque. Mientras que los drones de reconocimiento carecen de actuadores específicos y simplemente recogen información (básicamente visual y de geolocalización) durante su vuelo para su posterior análisis, los drones de ataque sí que poseen actuadores específicos incluyendo munición o cargas explosivas que el dron puede lanzar sobre los objetivos o bien activar durante una caída autodestructiva. En este último caso, hablamos de los llamados de drones kamikazes.

Por otra parte, y por lo que respecta al control de los drones militares, podemos hablar de drones controlados a distancia, de drones que rondan, de enjambres de drones, de drones de ataque semiautónomos y de drones autónomos:

1. Los drones controlados a distancia, sean de reconocimiento o de ataque, están en permanente contacto con un operador en tierra, que los dirige y conduce a distancia mientras observa en pantalla la información que captan sus cámaras y sensores. Si hay que consumar un ataque (*In the Loop Drones*), el operador es quien selecciona el objetivo, toma la decisión de atacar, y ordena el ataque. El dron, eso sí, puede (y suele) estar dotado de sistemas de seguimiento automático que van persiguiendo de forma automática el objetivo una vez este ha sido identificado por el operador.
2. Los drones que rondan (*Loitering* en inglés) no están dirigidos a un determinado objetivo, sino que van sobrevolando una determinada zona. Tras especificar esta región de interés, el operador deja que el dron vaya vagando y volando por ella, captando información de todo aquello que encuentra. Estos drones pueden ser también de reconocimiento o de ataque. En el primer caso, simple-

mente transmiten la información captada a la base. En el caso de estar preparados para el ataque, si actúan por control a distancia pasan a funcionar como los drones del apartado 1 siguiendo las instrucciones del operador. En caso contrario, nos encontramos en los supuestos 4 ó 5.

3. Los enjambres de drones (*Drone Swarms*) son conjuntos de decenas, centenares o miles de mini drones que actúan coordinadamente gracias a un sistema específico de comunicación que posibilita la interacción entre ellos. También pueden ser armados, de reconocimiento o enjambres que rondan. Son objeto de investigación por parte de varios países, y también potenciales candidatos a incluir capacidades autónomas. Se inspiran en el comportamiento de los enjambres de pájaros y son extraordinariamente resistentes a los accidentes y adversidades porque, en el caso de problemas, cualquier subconjunto de drones del enjambre puede continuar desarrollando las tareas asignadas. Por lo demás, funcionan como los drones en 1 ó 2.
4. Los drones de ataque semiautónomos (*On the Loop Drones*) son drones de cualquiera de los tipos anteriores (1, 2 ó 3) que incluyen, además de los sistemas de captación, de localización e identificación de objetivos, de seguimiento de estos objetivos y de ataque destructivo, un sistema de decisión que se supone que, dada una lista de objetivos potenciales ya identificados, “decide” si alguno de ellos debe ser atacado. En caso afirmativo, lo comunica al operador, quien dispone de un cierto tiempo, habitualmente limitado, para o bien aceptar la propuesta del dron y atacar, o bien descartar el ataque.
5. Los drones armados autónomos (AWS, también clasificados como *Out of the Loop Drones* porque desaparece la intervención humana del proceso de identificación de objetivos y decisión de ataque) son una evolución de los anteriores drones de tipo 4 que elimina toda consulta al operador y actúa en base a lo que indican sus algoritmos. Dado que la mayoría (no todos) de los desarrollos en este campo se basan en técnicas de inteligencia artificial, los trataremos en un apartado específico.

## Los ataques a distancia

La historia de los sistemas militares de ataque ha sido también la de la conquista de la distancia. La distancia al enemigo genera superioridad e incrementa la seguridad del atacante, porque mantiene la posibilidad de destruir los objetivos re-

duciendo riesgos durante el ataque. Las flechas fueron más seguras (siempre desde el punto de vista de los atacantes) que las lanzas y espadas, y las armas de fuego lo fueron más que las flechas. Luego llegó la artillería, los bombardeos aéreos y los misiles. La tecnología militar ha ido proponiendo sistemas de ataque cada vez a mayor distancia.

En todo caso, las últimas décadas has visto un cambio cualitativo en este sentido, como las bombas guiadas por láser y los drones controlados a distancia ya comentados. En el primer caso, las bombas guiadas son proyectiles explosivos que pueden corregir y afinar su trayectoria una vez han sido disparados o lanzados (habitualmente desde un avión), dirigiéndose a objetivos que el operador va señalando en tiempo real con un láser. En el caso de los drones controlados a distancia, en cambio, su operador puede encontrarse a miles de kilómetros, viendo en tiempo real tanto su localización como lo que van captando sus sensores y cámaras. El operador de los drones los va pilotando desde el ordenador de la mesa de su despacho, que puede estar a más de 10.000 kilómetros del dron, y en cualquier momento puede ordenar el ataque y destrucción del objetivo.

**Cuando las operaciones militares se realizan a través de una cámara de video lejana, como en los drones guiados, la percepción de daños disminuye**

Los componentes tecnológicos que permiten el control de los drones a distancia incluyen los sistemas de comunicación y de seguridad y encriptación de los datos. Todos ellos, componentes de doble uso con la única característica específica de usar satélites militares de comunicación. En el caso de las bombas guiadas, los componentes tecnológicos incorporan cámaras de detección de la señal láser y sistemas automáticos y adaptables de vuelo.

La diferencia entre uno y otro caso es doble: la distancia y la percepción del objetivo. En las bombas guiadas (usadas por primera vez en la guerra del Golfo de 1991), el operador militar ve el objetivo real mientras utiliza el láser como un puntero letal que va marcando el blanco a la bomba. En cambio, en el caso de los drones controlados a distancia, esta distancia es enormemente mayor; además, la percepción del entorno a atacar queda mediatizada por la pantalla del ordenador, los sistemas de comunicación, los de seguimiento y los de procesamiento de imagen. Todos ellos pueden introducir ruido, modificaciones y perturbaciones que limitan la capacidad de decisión objetiva del operador.

En este sentido, autoras como Medea Benjamín consideran que cuando las operaciones militares se llevan a cabo a través del filtro de una cámara de video lejana, la posibilidad de contacto visual con el enemigo desaparece, con lo cual la percepción de los daños del posible ataque a personas disminuye.<sup>5</sup> Por otro lado, Markus Wagner explica que la desconexión y la distancia crean un entorno en el que es más fácil cometer atrocidades.

Una última consideración relacionada con los drones controlados a distancia (tipos 1 a 4 en la clasificación presentada anteriormente) tiene que ver con el llamado *sesgo de automatización*. Se ha demostrado que los humanos tendemos a seguir las indicaciones de las máquinas sin comprobar la verosimilitud de sus propuestas. En este sentido, las perturbaciones que los sistemas de comunicación a distancia pueden introducir en lo que observa el operador militar pueden llevarle a tomar decisiones erróneas.

## Los sistemas de inteligencia artificial

En los drones y otros sistemas militares armados y autónomos (de tipo 5 en la anterior clasificación) debemos distinguir entre autonomía constructiva y autonomía de uso. La constructiva significa que el sistema tiene la capacidad de actuar y atacar autónomamente, aunque en muchos casos esta capacidad no se utilice y en cambio se dirija a distancia. Como ejemplo tenemos el dron Israelí Harop, que puede actuar, según el tipo de software que se le active, en modo controlado o en modo autónomo.<sup>6</sup> La autonomía de uso aparece cuando las personas responsables de su despliegue deciden que estos sistemas de ataque actúen sin intervención humana alguna.

La inteligencia artificial es un concepto muy amplio que incluye una gran variedad de técnicas y algoritmos. Una definición bastante clarificadora es la que señala que es la inteligencia que pueden llegar a tener las máquinas, realizando tareas

---

<sup>5</sup> Brunet, Font, Mojal y Rodríguez, 2019, *Op. cit.*, p. 23.

<sup>6</sup> «Autonomous weapons and the new laws of war», *The Economist*, Briefing, enero de 2019. Disponible en: <https://amp.economist.com/briefing/2019/01/19/autonomous-weapons-and-the-new-laws-of-war>. En relación a los drones Harop, FireFly, Kargu-2 y Qasef-1 véase también Paul Iddon, «Turkey, Israel And Iran Have Built Some Very Lethal Loitering Munitions», *Forbes*, 19 de julio de 2020. Disponible en: <https://www.forbes.com/sites/pauliddon/2020/07/19/turkey-israel-and-iran-have-built-some-very-lethal-loitering-munitions/amp/?streamIndex=1>



que típicamente requieren el uso de capacidades humanas inteligentes.<sup>7</sup>La inteligencia artificial es, por tanto, “inteligencia” de máquinas, y se basa en la posibilidad de actuar, en el marco de determinadas tareas, de manera parecida los humanos. Se trata de una “habilidad” para realizar y resolver tareas, captando la realidad con sensores y luego actuando. En este sentido, no incluye la posibilidad de razonar ni de pensar.

Durante las últimas décadas la inteligencia artificial (IA) se ha ido materializando básicamente en nuevos algoritmos denominados de aprendizaje automático profundo (*Deep Learning*, DL, en inglés) Estos sistemas primero deben aprender de un número ingente de datos antes de empezar a actuar. Para aprender, necesitan grandes cantidades de información. No puede haber sistemas de inteligencia artificial basados en aprendizaje profundo sin *big data*. Al final de este proceso de aprendizaje o entrenamiento, que se hace en grandes ordenadores, la red neuronal acaba teniendo sus millones de parámetros ajustados en base a los datos de entrenamiento y puede ser ya instalada en el sistema o artilugio que la utilizará en la práctica. El aprendizaje podríamos decir que construye la red neuronal, porque “aprende” de los datos y “personaliza” los parámetros de todas sus conexiones. Luego, esta red, en dispositivos y ordenadores mucho más modestos, recibirá datos (por ejemplo, imágenes), los filtrará y procesará en la red entrenada, y generará determinados resultados (proponiendo, por ejemplo, qué personas en la imagen de entrada podrían ser sospechosas).<sup>8</sup>

**Los sistemas de IA son poco fiables. Por eso, nunca deberían utilizarse en aplicaciones críticas sin supervisión humana**

Los sistemas de IA son no fiables, con una probabilidad garantizada de error que no es despreciable. Por ello, nunca deberían utilizarse en aplicaciones críticas sin supervisión humana. Ello se aplica, obviamente, a los sistemas militares de armamento.

<sup>7</sup> Stuart Russell y Peter Norvig, «Artificial Intelligence: A Modern Approach», Prentice Hall, 4ª ed., última modificación: 9 de junio de 2021. Disponible en: <http://aima.cs.berkeley.edu>

<sup>8</sup> Para más información sobre los sistemas de inteligencia artificial así como sobre su utilización militar y los problemas éticos que ello supone, ver: Pere Brunet, Tica Font, Joaquín Rodríguez, *Robots Asesinos, 18 preguntas y respuestas*, Campaña SKR, Centro Delàs y UAB, 2021. Disponible en: [http://centredelas.org/wp-content/uploads/2021/12/RobotsAsesinos\\_18PreguntasYRespuestas\\_DEF.pdf](http://centredelas.org/wp-content/uploads/2021/12/RobotsAsesinos_18PreguntasYRespuestas_DEF.pdf)

## Otros sistemas de doble uso

Además de los ya citados, nos encontramos con una larga lista de componentes tecnológicos de uso civil que también incorporarán los nuevos sistemas militares. Entre ellos podemos citar todo tipo de cámaras y sensores, las técnicas de reconocimiento a partir de imágenes (utilizados también en muchos escenarios cotidianos), los sistemas de procesamiento y mejora de imágenes, los de navegación y geolocalización, los sistemas de defensa contra ciberataques, los elementos y algoritmos de control de vuelo (necesarios en los sistemas no tripulados de reconocimiento y ataque pero también en los drones de uso civil), las redes (internet y wifi), la seguridad en las comunicaciones y encriptación de los datos, e incluso los sistemas de protección y camuflaje para prevenir daños tanto en la población civil como en los combatientes.

Algunos de estos sistemas, como los de control y reconocimiento facial con cámaras, están actualmente en el centro del debate ético, incluso en el campo de las aplicaciones civiles. Lo están por su probable vulneración de los derechos fundamentales de las personas, pero también por su porcentaje de errores, que no es nada despreciable.

En todo caso, uno de los problemas que veremos asociados a estos nuevos componentes tecnológicos es el de la difuminación de la frontera entre lo civil y lo militar por la creciente facilidad de fabricación artesanal de armamento y sistemas sofisticados de ataque. A la posibilidad ya real de construir armas de fuego caseras con sistemas comerciales de impresión 3D se añade ahora, por ejemplo, la de crear sistemas de reconocimiento o de modificar drones de uso civil para finalidades agresivas.

## Los mismos perros, con collares más atractivos

La espiral belicista se alimenta de los valores patriarcales y de los intereses del complejo militar-industrial, así como de los nuevos desarrollos tecnológicos. El objetivo actual de la mayoría de Estados del mundo es continuar armándose para la guerra, pero haciéndolas más asequibles y con un coste menor. En otras palabras, se pretende que las guerras del próximo futuro sean más “limpias” y baratas, sin reducir, claro está, su poder destructivo. Y lo cierto es que, una vez desarrolladas

estas nuevas tecnologías, proliferarán ampliamente, con el peligro de que todo esto impulse una nueva carrera armamentística.

La inteligencia artificial y los avances en nuevas tecnologías harán más fácil pensar en la guerra en abstracto, y ello dificultará evitar los conflictos armados. Zeng Yi, alto ejecutivo de la tercera compañía de defensa más grande de China, en el Foro Xiangshan de octubre de 2018 predijo que en 2025 las armas autónomas letales serían habituales, y dijo: «En los futuros campos de batalla no habrá gente que luche [...] el uso militar de la IA es cada vez más inevitable. Estamos seguros de que este será el futuro».<sup>9</sup>

Una de las razones para esta escalada tecnológica militar se basa en la competitividad: si lo hacen los otros, lo tenemos que hacer nosotros, para no quedarnos atrás. Triste argumento. Porque los riesgos a largo plazo que plantea la proliferación y el desarrollo de estos sistemas de armamento superan los pretendidos beneficios a corto plazo que pueden parecer tener. En efecto:

- Los nuevos sistemas militares de ataque, de menor coste, disminuirán el riesgo económico de las operaciones militares.
- Los sistemas militares robóticos rebajarán los umbrales de las acciones militares por una supuesta carencia de riesgo de muerte. En consecuencia, los Estados podrían estar más dispuestos a atacarse mutuamente. Todo ello puede verse agravado por la asimetría de fuerzas que estos sistemas propiciarán.
- Estos sistemas harán más probables las percepciones erróneas, las decisiones incorrectas y la escalada involuntaria de los conflictos.
- Muchos de estos sistemas acabarán proliferando y llegando a una amplia variedad de actores, de forma que la ventaja militar inicial que estos sistemas pueden dar a los países actualmente líderes en este campo será temporal. Pequeños países y organizaciones de todo tipo sabrán convertir drones comerciales en drones armados, con alto peligro para personas no involucradas en conflictos.
- Las escalas de tiempo en los conflictos armados serán más rápidas de lo que los humanos pueden percibir, socavando la capacidad de los seres humanos para tomar decisiones responsables durante las operaciones militares. Los sistemas de armamento autónomo diseñados e implementados por fuerzas opuestas podrán reaccionar e interactuar entre sí de manera descontrolada.

<sup>9</sup> Brunet, Font, Mojal y Rodríguez, 2019, *Op. cit.*, p. 39.

- La imprevisibilidad y los errores inherentes a estos nuevos sistemas producirán sin duda un mayor número de muertes civiles.
- Finalmente, no debemos descartar la potencialidad de alterar los equilibrios geopolíticos abriendo una nueva era de inestabilidad global que podría abocarnos a nuevas guerras.

Y un último apunte: los Estados Unidos, además de continuar su carrera armamentística diversificada en campos que cubren desde los misiles balísticos hasta los drones y las armas nucleares, han iniciado programas avanzados como el de la fuerza espacial. Aunque los inicios de esta fuerza se sitúan en los comienzos de la Guerra Fría, no fue hasta 2001 cuando la Comisión Espacial abogó por la creación de un cuerpo espacial que estuvo gestándose entre 2007 y 2019 hasta concretarse en la Ley de la Fuerza Espacial de 20 de diciembre de 2019. En su informe de agosto de 2020, *Spacepower: Doctrine for Space Forces*, se indica que el poderío espacial es vital para la prosperidad y la seguridad de los EUA. Todavía es pronto para saberlo, pero habrá que estar atentos a los desarrollos tecnológicos asociados a este proyecto.

La comunidad internacional debería, como mínimo, prohibir el desarrollo, despliegue y uso de sistemas no tripulados autónomos y armados, así como las armas espaciales robóticas y los sistemas no tripulados provistos de armas nucleares como paso previo a una progresiva desmilitarización a nivel mundial.

**Pere Brunet** es miembro del Centro Delàs de Estudios por la Paz

