USOS HOSTILES DE SISTEMAS ROBÓTICOS Y AUTÓNOMOS POR ACTORES NO ESTATALES

EVA MARTÍN IBÁÑEZ

DOCTORA EN CIENCIAS DE LA INFORMACIÓN

RESUMEN

Los sistemas robóticos y autónomos (RAS) hacen más fácil, más seguro y más barato que personas no expertas realicen labores de vigilancia y adopten nuevas tácticas y armas. Los usos hostiles de esos sistemas están protagonizados por una amplia variedad de actores, tanto colectivos como individuales, con motivaciones muy diversas. En la última década, se han reducido las barreras de entrada para acceder a sistemas no tripulados debido a la creciente oferta comercialmente disponible. Cuando las condiciones son adecuadas, el empleo de sistemas robóticos y autónomos puede ser factible para cualquier actor no estatal.

Palabras clave: robótica, sistemas robóticos y autónomos, sistemas no tripulados, drones, actores no estatales

ABSTRACT

Robotic and Autonomous Systems (RAS) make it easier, safer and less expensive for non-experts to carry out surveillance tasks and to embrace new tactics and arms. A wide range of non-state actors (groups and individuals), with different motivations, resort to hostile uses of those systems. In the last decade, barriers to entry unmanned systems had lowered, due to the growing commercially available offer. Under the right conditions, any non-state actor can make use of robotic and autonomous systems.

Keywords: robotics, robotic and autonomous systems, unmanned systems, drones, non-state actors

1. INTRODUCCIÓN

Los sistemas robóticos y autónomos (RAS) ponen en manos de todo tipo de grupos e individuos capacidades que antes estaban reservadas a las fuerzas armadas. Hacen más fácil, más seguro y más barato que personas no expertas realicen labores de vigilancia y adopten nuevas tácticas y armas, incluyendo las de destrucción masiva.

Los primeros casos de usos hostiles de sistemas no tripulados datan de hace más de veinte años, aunque su empleo se ha acentuado en la última década. Dichos usos suceden en todos los dominios: aire, mar y tierra. Sin embargo, los aéreos son los más utilizados, por la mayor cantidad y variedad de modelos disponibles comercialmente y porque ofrecen mayores prestaciones que sus homólogos terrestres y marítimos.

Del análisis de los casos documentados, se deducen las capacidades ya alcanzadas por los actores no estatales en el uso de sistemas no tripulados: inteligencia,

vigilancia y reconocimiento (ISR); mensajería; propaganda; armado (artefactos explosivos improvisados (IED), armas biológicas, químicas y radiológicas, cohetes, misiles y armas de fuego); tráfico de mercancías ilegales e ilícitas; transporte (logística y aprovisionamiento); e inteligencia electrónica. Según esos actores adquieran experiencia, se prevén usos novedosos y técnicamente avanzados.

Las páginas siguientes están dedicadas a definir varios conceptos clave: robots, sistemas no tripulados, sistemas robóticos y autónomos y actores no estatales. A continuación se indaga en por qué estos sistemas son atractivos para los actores maliciosos, seguido de los motivos de preocupación que suscitan.

Posteriormente, se analiza el uso de sistemas robóticos y autónomos por parte de actores no estatales como una práctica de ingeniería compleja. Asimismo, se muestra que los usos hostiles de sistemas robóticos y autónomos se pueden producir en todos los dominios. Después, el apartado sobre posibles desarrollos futuros recoge las tendencias potenciales y, por último, están las conclusiones.

2. DEFINICIONES PRELIMINARES

Antes de iniciar el análisis, incluimos las definiciones de varios conceptos: robots, sistemas no tripulados, sistemas robóticos y autónomos (RAS), y actores no estatales.

Un robot es una máquina alimentada capaz de ejecutar una serie de acciones mediante control humano directo, control por ordenador o una combinación de ambos. Comprende un sistema de plataforma, un software y una fuente de energía (US Army, 2016, p. 21).

En defensa y seguridad es habitual el uso del término sistema no tripulado (*unmanned system*), que es una plataforma aérea, terrestre, de superficie, bajo superficie o espacial que no tiene un operador humano físicamente a bordo (US Army, 2016, p. 22).

A menudo la palabra drones se utiliza indistintamente con sistemas no tripulados. Además, suele ser frecuente el uso de siglas. Para referirse a los sistemas aéreos no tripulados, son comunes UAS (*Unmanned Aerial System*) y REPAS (*Remotely Piloted Aircraft System*). Los terrestres son conocidos como UGS (*Unmanned Ground System*), y los marítimos como UMS (*Unmanned Maritime System*) en general, o también por USS (*Unmanned Surface System*) para los marítimos de superficie y por UUS (*Unmanned Underwater System*) para los submarinos. Para aludir a todos estos sistemas no tripulados también se emplea UxS o simplemente US (*Unmanned Systems*).

La tendencia actual es prescindir del calificativo no tripulado. Uno de los motivos es que induce a confusión, porque, a pesar de la ausencia de un operador a bordo, esos sistemas no están exentos de la intervención de seres humanos, especialmente de personal de apoyo. Por ejemplo, para operar un solo Predator como patrulla aérea de combate durante veinticuatro horas hace falta una plantilla de 168 personas, y un Reaper requiere 171 personas (Cockburn, 2015, p. 146, 179).

Los sistemas robóticos y autónomos o RAS (*Robotic and Autonomous Systems*) son aquellos que tienen un elemento robótico, un elemento autónomo o, frecuentemente, ambos (US Army, 2016, p. 21). Es un término que está ganando difusión en el ámbito de la defensa y la seguridad y que empieza a sustituir al de sistemas no tripulados.

Un actor no estatal es cualquier entidad que no es un Estado según el Derecho Internacional. En sentido amplio, la tipología comprende organizaciones intergubernamentales, organizaciones no gubernamentales, corporaciones multinacionales y grupos tales como grupos rebeldes, organizaciones terroristas, grupos religiosos, organizaciones de la sociedad civil, empresas e incluso individuos (Kyriakopoulos, 2016, p. 52). En unos contextos, el término puede referirse a grupos sociales civiles benignos que promueven los derechos humanos. En otros, puede aludir a grupos incívicos que recurren a la violencia e incluso adquieren armas de destrucción masiva. Todos ellos tienen el potencial tanto de violar como de fomentar los derechos humanos (Clapham, 2016, pp. 1-2).

Los actores no estatales violentos son aquellos grupos armados no estatales que recurren a la violencia organizada como herramienta para conseguir sus objetivos. No son inherentemente buenos o malos, ni están inherentemente opuestos al Estado. Algunos, como las compañías militares privadas y los actores de contra-oposición, a menudo se encuentran en el mismo bando del conflicto que el Estado. Por ese motivo, conviene estudiarlos como un todo, en lugar de centrarse solo en aquellos que aplican tipos específicos de violencia, como el terrorismo y las insurgencias (Gartenstein-Ross, 2014, p. 48).

El término actores no estatales violentos requiere una urgente clasificación. Demasiado a menudo se identifica a los actores no estatales violentos con grupos “terroristas”, pero eso simplifica en exceso su función (Gartenstein-Ross & Zenn, 2017).

Para categorizar a los actores no estatales violentos más relevantes en la actualidad, Gartenstein-Ross y Zenn (2017) proponen una clasificación articulada según su relación con el Estado, como muestra la Tabla 1.

Terrorismo e insurgencias	Criminalidad	Ciber	Grupos de interés	Status quo
Terroristas. Insurgentes. Insurgentes plus.	Traficantes. Bandas. Cárteles.	Actores no estatales que solo operan en el ciberespacio	Grupos de autoprotección. Señores de la guerra. Agentes de poder local	Actores de contra-oposición. Actores no estatales patrocinados por Estados. Compañías militares privadas. Mercenarios

Tabla 1. Tipología de actores no estales violentos. Fuente: Adaptado a partir de Gartenstein-Ross & Zenn, 2017.

La posición, de izquierda a derecha, refleja el grado de cercanía del actor no estatal violento con el Estado, con espectros de colores que van desde el rojo (más lejano al Estado) al azul (más cercano), pasando por el naranja, el amarillo y el verde.

- Terrorismo e insurgencias

El espectro rojo engloba a aquellos actores que buscan derrocar, debilitar o conseguir concesiones de los actores estatales. La mayoría de los terroristas pretenden provocar una reacción exagerada del Estado contra la comunidad que dicen representar. Por su parte, las insurgencias desean ganar el control de un territorio. La categoría de

insurgencia plus se refiere a aquellos actores que presentan cualidades similares a los Estados, por ejemplo, Daesh. El cambio más notable en la dinámica de este tipo es el creciente uso innovador de los medios sociales de Internet, que les permite conseguir un alcance transnacional rápidamente (Gartenstein-Ross & Zenn, 2017).

- Criminalidad

El espectro naranja incluye traficantes, bandas y cárteles. Suelen operar contra la ley del Estado, pero, a diferencia de terroristas e insurgentes, generalmente no suelen buscar una guerra con el Estado, dado que su principal motivación es económica. Las bandas despiertan preocupación en el hemisferio occidental, porque causan patrones de inmigración irregular (Gartenstein-Ross & Zenn, 2017).

- Ciber

El espectro amarillo está compuesto por actores no estatales violentos que solo operan en el ciberespacio. Pueden considerarse violentos porque amenazan con la violencia; actos como desvelar información personal sin consentimiento (*doxing*) pueden entrar en esa definición (Gartenstein-Ross & Zenn, 2017).

- Grupos de interés

Los actores dentro del espectro verde (grupos de auto-protección, señores de la guerra, y agentes de poder local) suelen mantener unas relaciones neutrales e incluso positivas con los Estados. Los grupos insurgentes y terroristas pueden representar una mayor amenaza para los actores de este tipo que para el Estado (Gartenstein-Ross & Zenn, 2017).

- Status quo

El espectro azul engloba a aquellos actores que tienden a alinearse explícitamente con el Estado contra otros actores no estatales violentos. Incluye los de contra-oposición[1], los patrocinados por Estados, las compañías militares privadas, y los mercenarios (Gartenstein-Ross & Zenn, 2017).

Las actividades de los actores no estatales armados son uno de los principales riesgos para la paz y la estabilidad mundiales. “Vigilantes, grupos sectarios, empresas privadas de seguridad, bandas criminales, milicias, guerrilleros o insurgentes” son “un tema recurrente” en los “asuntos de seguridad internacional” (Laborie, 2015, p. 41).

3. EL ATRACTIVO DE LOS SISTEMAS ROBÓTICOS Y AUTÓNOMOS

El interés de los terroristas por los drones no es un fenómeno nuevo; se remonta a más de veinte años[2]. Sin embargo, su uso se ha hecho más frecuente en la última

1 Los actores de contra-oposición suelen surgir en un conflicto concreto, y suelen estar organizados teniendo en cuenta un adversario específico, pero no forman parte del ejército estatal (Gartenstein-Ross, 2014, p. 51),

2 El primer caso conocido que expresa el interés de un grupo terrorista en los drones ocurrió entre finales de 1993 y principios de 1994 en Japón e involucra a la secta apocalíptica Aum Shinrikyo, responsable del atentado con gas sarín de 1995 en el metro de Tokio.La organización estuvo experimentando con un par de helicópteros teledirigidos como los de fumigar cosechas, que se estrellaron durante las pruebas (Rassler, 2016, pp. 13-14).

década, sobre todo el de las variantes de drones comercialmente disponibles, que cada vez son más populares, sofisticados y accesibles. De todos modos, aunque muchos grupos e individuos han mostrado inclinación hacia estos sistemas no tripulados, muy pocos han tenido éxito a la hora de desplegarlos. Su impacto todavía es muy limitado (Rassler, 2016, pp. IV-V).

Las ideologías de los actores no estatales interesados en utilizar drones son diversas. Aunque gran parte de los casos registrados están inspirados por concepciones radicales islamistas, también hay entidades motivadas por ideologías apocalípticas, irrederentistas o de extrema derecha (Rassler, 2016, p. V).

Los sistemas robóticos y autónomos resultan atractivos para los actores no estatales (colectivos e individuales) por los beneficios que otorgan. Ofrecen capacidades que pueden aumentar significativamente el impacto de un ataque y las probabilidades de éxito. La Tabla 2 resume esos beneficios.

- Permiten actuar contra objetivos lejanos manteniéndose a distancia, incluso desde fuera de las fronteras o desde el mar.
- Costes de adquisición relativamente bajos y facilidad de transporte.
- Múltiples aplicaciones y diversidad de cargas (sensores y ofensivas).
- Eficaces herramientas de inteligencia, vigilancia y reconocimiento (ISR).
- Mayor intimidad y cercanía al objetivo para ataques de precisión.
- Gran flexibilidad en ataques indirectos adicionales (para sembrar el caos y para redirigir personas hacia o fuera de un lugar específico).
- Merodeo sobre el objetivo durante largos periodos de tiempo.
- En algunos sistemas, cuando el operador humano queda comprometido, es posible pasar a un modo de ataque completamente autónomo.
- Disminuir el riesgo de captura del operador (según el método de control del robot).
- Reducir el coste de los ataques (accesibles a actores individuales y grupos pequeños).
- Circunvalar las defensas del perímetro desafiando la seguridad física.
- Orquestar múltiples ataques simultáneos para aumentar el efecto de las operaciones.
- Campañas prolongadas de ataque con efectos sostenidos que erosionen la confianza y causen interrupciones y perturbaciones.
- El propio robot como arma (similar a terrorista suicida o artefacto explosivo improvisado).
- Dispersar armas no convencionales (nucleares, biológicas, químicas y radiológicas).
- Ciertos sistemas pueden realizar ataques coordinados en enjambre, capaces de arrollar las defensas.
- Defensa contra ataques de otros drones de fuerzas adversarias.
- Transporte de materiales (logística y abastecimiento).
- Tráfico de mercancías ilegales e ilícitas.
- Alto valor simbólico de los drones (ganar prestigio).
- Mensajería y comunicaciones estratégicas (mensajes y documentos).
- Medios para documentar y publicitar el potencial de dañar y asesinar (propaganda).
- Interceptar o interferir comunicaciones electrónicas.
- Recopilar datos explotables en operaciones de guerra psicológica.
- Fórmulas de perturbación (acoso, protesta o vandalismo).

Tabla 2. Beneficios de los sistemas no tripulados para los actores no estatales. Fuente: Elaboración propia.

Los sistemas no tripulados comercialmente disponibles en la actualidad presentan una serie de especificaciones relevantes que afectan a sus posibles usos hostiles y criminales, que están reseñadas en la Tabla 3.

Vehículos aéreos no tripulados (UAV)	
Carga	La mayoría de los UAV comerciales puede cargar un cardán, una cámara y una batería. Aquellos con mayor capacidad pueden transportar otros dispositivos de captura de imágenes como un LiDAR o una cámara infrarroja.
Alcance	Los modelos comerciales suelen estar limitados por la transmisión de señales, la distancia de retransmisión de imágenes y la autonomía de la batería. Así, el piloto debe estar cerca.
Resistencia	La habilidad de operar en condiciones meteorológicas adversas, como viento fuerte, lluvia o nieve, está reservada a pocos modelos de precio elevado. Los usuarios pueden mejorar la resistencia, pero a costa de añadir peso, lo que reduce el tiempo de vuelo y lastra la carga, salvo que se aumente la potencia o el número de rotores.
Imágenes	Son comunes las cámaras de alta resolución, capaces de tomar fotos y vídeos. El uso de un cardán posibilita el giro electrónico de la cámara. También se pueden instalar cámaras infrarrojas y LiDAR.
Pilotaje automático	Muchos drones comerciales permiten programar una ruta de vuelo mediante coordenadas GPS. Los más modernos incluyen funciones de autopilotaje y de seguimiento del operador.
Vehículos marítimos no tripulados (UMV)	
Carga	La capacidad de carga se ve afectada por el espacio interior y la flotabilidad. Una carga que supere el peso de flotabilidad hará que el UMV se hunda en proporción a la varianza de peso. Cualquier espacio libre en la cámara de carga de un UMV submarino se puede llenar con espuma flotable para aumentar el peso de la carga potencial. Los modelos de baja gama pueden carecer de capacidad de carga.
Alcance	El alcance de los UMV no está determinado por el rango de control, si es capaz de comunicarse por satélite o por GPS. Entonces, los factores determinantes son la capacidad del combustible (generalmente baterías eléctricas) y la velocidad óptima. Sin GPS, el UMV suele estar limitado por el alcance del controlador Wi-Fi (unos 300 m) o por la conexión por cable físico con el piloto (generalmente menos de 100 m).
Imágenes	Los dispositivos de imágenes suelen estar instalados en la cámara de carga. Pueden ser instrumentos científicos para medir la presión o la calidad del agua, sonar y dispositivos visuales. Eso posibilita la vigilancia y el reconocimiento.
Velocidad	La velocidad depende de la potencia del motor y de la forma y el peso de la nave. Es clave en los UMV de superficie, que suelen alcanzar velocidades de hasta 50 km/h. En cambio, los submarinos no tripulados son mucho más lentos (entre 5 y 10 km/h).
Profundidad	El casco de un UMV determina la profundidad. Aquellos con cascos hechos de metales resistentes, como el titanio, pueden descender a mayores profundidades que los de plástico o metales baratos. La profundidad no afecta en las misiones contra objetivos sobre la superficie del agua, pero ciertos objetivos de infraestructuras críticas están a grandes profundidades, como oleoductos, plataformas petrolíferas y cables de comunicaciones.
Vehículos terrestres no tripulados (UGV)	
Carga	La capacidad de carga de los UGV varía mucho. Como sucede con la mayoría de los vehículos no tripulados, mayor velocidad y movilidad implican cargas menores.
Alcance	La mayoría de los UGV controlados a distancia tiene un alcance limitado, pero los modelos de alta gama se pueden configurar para misiones específicas. El alcance que un operador hostil puede necesitar depende del nivel de riesgo al que quiera exponerse. En la práctica, el alcance efectivo también está en función del tipo del terreno que el vehículo tengan que recorrer.
Imágenes	Los UGV pequeños proporcionan información situacional limitada a los operadores, comparados con los UAV. Sin sistemas de telemetría, la navegación basada solo en la retransmisión de vídeo reduce mucho la efectividad. Aquellos UGV equipados con sensores ambientales avanzados, como cámaras térmicas o sensores químico-biológicos, ofrecen a los operadores una mayor comprensión del terreno.
Movilidad y velocidad	Los UGV pueden desplazarse por diversos terrenos en varios modos y configuraciones. La capacidad de moverse por todos los terrenos (colinas, obstáculos, áreas semiacuáticas y superficies irregulares) influye en su velocidad. A mayor capacidad de adaptarse a diversos terrenos, menor velocidad.

Tabla 3. Especificaciones relevantes que afectan a las operaciones de los sistemas no tripulados hostiles actuales. Fuente: Elaboración propia a partir de Open Briefing, 2016, p. 5-9.

El mercado de los vehículos aéreos no tripulados (UAV) ha crecido significativamente en los últimos cinco años. Es evidente el liderazgo del sector comercial. Los

UAV comercialmente disponibles se venden en tres modalidades: listos para volar, con el transmisor personalizable, y con la posibilidad de personalizar el transmisor, el receptor, la batería y el cargador. Los modelos más comunes son los multicoptores con 4, 6 u 8 hélices. Los usuarios que buscan aumentar la capacidad de carga, el tiempo de vuelo y el alcance de los UAV es más probable que construyan drones personalizados a partir de componentes, lo que requiere conocimientos técnicos básicos (Open Briefing, 2016, p. 4-5).

Los vehículos marítimos no tripulados (UMV) engloban dos clases: submarinos y de superficie. Los más comunes son los submarinos, cuyas principales aplicaciones comerciales son la investigación marina y las actividades petrolíferas y gasísticas. Varios factores afectan a las operaciones de los UMV. Generalmente, los modelos de mayor precio tienen mayor capacidad de carga, más tecnologías de imagen, mayor alcance y mayor profundidad. El alcance y la profundidad de inmersión son las características operativas más importantes para los vehículos no tripulados submarinos. Por su parte, los de superficie dependen de la velocidad, la capacidad de carga y el alcance (Open Briefing, 2016, p. 8).

Los vehículos terrestres no tripulados (UGV) están disponibles desde hace varias décadas. El ejemplo más simple son los coches teledirigidos. En el otro extremo están los vehículos autónomos comerciales y la robótica militar avanzada actualmente en desarrollo. Existen dos categorías de UGV. En primer lugar, los vehículos controlados a distancia por humanos, que los conducen a distancia. La otras son los vehículos autónomos que conducen por sí mismos usando algoritmos, entradas de sensores y coordenadas GPS prefijadas. Solamente unas pocas especificaciones son comunes a todas las clases de vehículos terrestres no tripulado. La diversidad de tecnologías hace que sea complicado precisar los atributos operativos de los UGV (Open Briefing, 2016, p. 6-7).

Los sistemas robóticos y autónomos constituyen una tecnología de uso dual. Los destinados al mercado civil también se utilizan para fines menos benignos, como husmear, acosar, traficar con drogas y hacer contrabando en las prisiones. Aunque todavía existe un gran desfase entre las capacidades de los vehículos no tripulados militares y los civiles, los modelos comercialmente disponibles proporcionan a individuos, compañías y grupos hostiles capacidades que previamente solo estaban disponibles para el ejército (Open Briefing, 2016, p. 2, 3).

La Tabla 4 apunta los principales métodos que los actores no estatales pueden emplear para hacerse con un sistema robótico y autónomo que aporte capacidades asimétricas.

- Adquirir robots militares o policiales (comprándolos en el mercado negro, recibiéndolos de un Estado patrocinador o robándolos).
- Modificar robots comercialmente disponibles, obtenidos legal o ilegalmente (incluso al alcance de individuos particulares).
- Construir robots (por ingeniería inversa, mediante espionaje industrial o usando hardware y software comercialmente disponible en todo o en parte).
- Hackear un robot (por ejemplo, interceptando las comunicaciones o inyectando datos falsos) para interrumpir la misión, estrellarlo contra un objetivo o capturarlo con el fin de permutarlo, estudiarlo o incorporarlo al arsenal.

Tabla 4. Principales métodos de conseguir un robot que proporcione capacidades asimétricas. Fuente: Elaboración propia.

4. MOTIVOS DE PREOCUPACIÓN

Los vehículos no tripulados son un recurso clave de inteligencia, vigilancia y reconocimiento (ISR) para las organizaciones de defensa de los países desarrollados. Sin embargo, las barreras de entrada para fabricar sistemas no tripulados se han reducido, y grupos terroristas y organizaciones criminales son capaces de crear robots sofisticados usando componentes comerciales salidos de las estanterías. Con el fuerte crecimiento de los sistemas no tripulados en el aire, en el agua y bajo el agua, aumenta la amenaza de malos usos de esta tecnología (Patterson y Patterson, 2010, p. 1).

Según el uso de drones y otras tecnologías robóticas se haga más común, se espera que se difundan entre todos los miembros de la sociedad, tanto para lo bueno como para lo malo (Goodman, 2015, p. 291).

El último informe sobre riesgos globales del Foro Económico Mundial incluye la innovación tecnológica entre los cinco factores que exacerban los riesgos geopolíticos. En concreto, la innovación tecnológica aumenta el riesgo de conflicto. Una nueva carrera armamentística se está desarrollando con la robótica armada y la inteligencia artificial. El ciberespacio es un dominio conflictivo y el Ártico y los océanos profundos están abiertos al acceso de vehículos pilotados a distancia; en todos esos casos no existe un sistema establecido para regular un comportamiento responsable. Como son tecnologías de uso dual cuyo I+D sucede en el sector privado, se facilita la instalación de armas por parte de una mayor variedad de actores estatales y no estatales (World Economic Forum, 2016, p. 16).

Dos de las dinámicas más prominentes del siglo XXI son el crecimiento de la influencia sistémica de terroristas y otros actores no estatales violentos, y el advenimiento de una amplia variedad de tecnologías transformadoras. En el contexto de la seguridad internacional, el nexo de esas dos fuerzas es de especial preocupación, porque se teme que esos actores adopten tecnologías emergentes para aumentar la amenaza que presentan (Ackerman, 2016a, p. 1).

Gran parte de las preocupaciones de seguridad se centran en el hecho de que muchas tecnologías emergentes [como los sistemas robóticos y autónomos] hacen que sea más fácil, más seguro y más barato que personas no expertas adopten nuevas tácticas y armas, especialmente las de destrucción masiva (Ackerman, 2016a, p. 1).

Frente a esa situación son posibles dos actitudes extremas. Una es la tentación de engordar la amenaza, caracterizando a los actores no estatales violentos como supervillanos capaces de fabricar armas del apocalipsis, e ignorar las múltiples dificultades inherentes en tales iniciativas y los hechos empíricos de que en el pasado la mayoría de las veces esos actores son conservadores y imitadores en vez de innovadores en sus tácticas y armas. Otra actitud todavía más peligrosa es asumir que dichos actores nunca serán capaces de adoptar nuevas tecnologías, aún existiendo numerosos ejemplos de éxito (Ackerman, 2016a, p. 1).

El proceso de adopción y despliegue de tecnologías emergentes en su conjunto requiere una compleja aplicación práctica de conocimientos y materiales por los actores no estatales violentos. A la hora de evaluar la amenaza, gran parte del análisis consiste en ser capaces de juzgar correctamente el deseo y la capacidad de los adversarios para llevar a cabo operaciones de ingeniería compleja con éxito (Ackerman, 2016a, p. 1).

Los actores no estatales violentos pueden ejecutar complicados proyectos tecnológicos. Tales acciones se enfrentan a muchos obstáculos. Sin embargo, no hay que subestimar su habilidad para completar notables hazañas técnicas dirigidas a conseguir sus metas tácticas y estratégicas. Cuando las condiciones de la organización son adecuadas, casi cualquier tarea técnica, incluso las más complejas, son factibles para los actores no estatales violentos (Ackerman, 2016b, p. 133). Sin embargo, las mismas dificultades logísticas para proveerse de drones de última generación que afectan a algunos países también son aplicables a muchos actores no estatales (Horowitz, Kreps, y Fuhrmann, 2016, p. 32-33).

La preocupación por el uso de armas de destrucción masiva por actores no estatales está extendida en la comunidad internacional. Recientemente, el Consejo de Seguridad de Naciones Unidas aprobaba una resolución al respecto, durante la presidencia española. Es la Resolución 2325 de 15 de diciembre de 2016, que recoge un llamamiento a todos los países para fortalecer los controles nacionales que impidan la proliferación de armas nucleares, biológicas o químicas (NBQ) y de sus medios de distribución. El origen de la preocupación reside en la amenaza terrorista y en el riesgo de que actores no estatales puedan adquirir, desarrollar, traficar o usar armas NBQ y sus medios de entrega, incluyendo el uso de rápidos avances en ciencia, tecnología y comercio internacional para ese fin (United Nations, Security Council, 15 diciembre 2016).

La Resolución 2325 de 2016 no menciona expresamente los sistemas no tripulados. Sin embargo, sí lo hacía Jan Eliasson, vicesecretario general de las Naciones Unidas hasta el 31 de diciembre de 2016, en su discurso del 15 de diciembre de 2016 ante el Consejo de Seguridad sobre la proliferación de armas de destrucción masiva por actores no estatales: Tecnologías emergentes, como la impresión 3D y los vehículos aéreos no tripulados están aumentado las amenazas de un ataque con armas de destrucción masiva (Eliasson, 2016).

5. EL USO DE SISTEMAS ROBÓTICOS Y AUTÓNOMOS COMO INGENIERÍA COMPLEJA

El empleo de sistemas robóticos y autónomos (RAS) por actores no estatales violentos puede considerarse una práctica de ingeniería compleja. Esta perspectiva puede resultar útil para analizar los usos hostiles y criminales, especialmente cuando los actores mantienen actividades de carácter estable.

Un proyecto de ingeniería compleja por parte de un actor no estatal violento es aquel que cumple los siguientes requisitos:

- múltiples componentes o subtareas de distintos tipos que deben integrarse adecuadamente para que el proyecto tenga éxito;
- suele necesitar la participación de más de una persona [excepto en los supuestos de actores individuales];
- variedad de habilidades técnicas (por ejemplo, síntesis química, soldadura o electrónica); y
- un esfuerzo más sofisticado que las operaciones estándar para el contexto concreto de tiempo y lugar en el que opera el actor (Ackerman, 2016a, p. 2):

Terroristas, bandas, grupos de crimen organizado transnacional e insurgentes suponen una clase diferenciada de amenazas para la paz y la seguridad internacionales. Muy pocos son realmente globales por naturaleza (en alcance e influencia), igual que muy pocos Estados tienen capacidades globales. Pero muchos actores no estatales violentos no son simplemente locales o nacionales (Littlewood, 2016, p. i).

En la era de individuos empoderados y redes de organizaciones con acceso a tecnologías de información, conocimientos y materiales para perseguir y lograr sus objetivos, resulta tentador otorgar a esos actores el potencial de suplantar al Estado y a su autoridad legítima. Los Estados perdurarán; incluso los frágiles y fallidos raramente son destruidos o reemplazados por actores no estatales violentos. Sin embargo, los Estados no son siempre los únicos actores, ni los más poderosos en cualquier localidad o región (Littlewood, 2016, p. i).

Existen casos que demuestran claramente que, a pesar de estar obligados a operar clandestinamente y enfrentándose a la presión de los cuerpos y fuerzas de seguridad, varios actores no estatales violentos han demostrado que son capaces de realizar tareas de ingeniería verdaderamente sorprendentes (Ackerman, 2016b, p. 119).

El estudio de casos de prácticas de ingeniería compleja por parte de actores no estatales violentos como la secta apocalíptica japonesa Aum Shinrikyo, las FARC colombianas, los Zetas, Hamas y AQ Khan permite encontrar similitudes en los procesos de decisión, implementación y obtención de resultados (Ackerman, 2016b, p. 120-131). Del análisis de esos casos, pueden deducirse dos características comunes que influyen en la decisión: En todos los supuestos un líder de la organización como mínimo ha dado el visto bueno y además existe una alta tolerancia al riesgo entre los decisores (Ackerman, 2016b, p. 120).

Hay cuatro factores que aumentan la probabilidad de que los actores no estatales violentos completen con éxito un programa de ingeniería compleja (Ackerman, 2016b, p. 129-130): recursos humanos y financieros, experiencia técnica, santuario, y cultura de aprendizaje, como muestra la Tabla 5.

1) **Recursos de inversión sustanciosos (humanos y financieros)**	No basta con que el actor tenga muchos recursos, sino que además debe querer y ser capaz de dedicar esos recursos al proyecto, manteniéndolos durante un extenso periodo de tiempo según el proceso de desarrollo madura.
2) **Experiencia técnica**	La adquisición o el desarrollo de conocimientos técnicos y de las habilidades requeridas es clave, ya proceda del exterior o se generen a partir de sus propios ensayos de prueba.
3) **Santuario**	Ser capaces de realizar actividades de investigación y desarrollo en un entorno relativamente seguro con un riesgo operativo relativamente bajo.
4) **Cultura de aprendizaje**	Perseverar hasta que se encuentra y ejecuta una solución para el problema. Está ligada a la inversión de recursos e implica el compromiso con el proyecto durante largos periodos de tiempo.

Tabla 5. Factores de éxito de los programas de ingeniería compleja por actores no estatales violentos. Fuente: Elaboración propia a partir de Ackerman, 2016b, p. 129-130.

En este sentido, ciertos indicadores potenciales pueden ser útiles para detectar e impedir las prácticas de ingeniería compleja por actores no estatales violentos. Uno son los cambios en el entorno estratégico o táctico que no se pueden compensar con una simple adaptación operativa o para los cuales no existen proveedores disponibles

de la tecnología necesaria. Otros son los intentos de esos actores de reclutar, contratar o coaccionar a especialistas, o cualquier otra manera de adquirir experiencia técnica (Ackerman, 2016b, p. 132).

A continuación. la Tabla 6 recoge algunos ejemplos de actores no estatales que desarrollan programas estables de sistemas robóticos y autónomos, como Hezbollah, Hamas y Daesh.

Hezbollah	Hezbollah es el grupo terrorista con el programa de UAS más sofisticado y antiguo, cuyos orígenes se remontan como mínimo a 1997. Se beneficia de sus estrechas relaciones con Irán. Muchos de los drones que Hezbollah ha operado durante la última década son versiones modificadas de sistemas no tripulados desarrollados por los iraníes con fines militares. En noviembre de 2004, un UAS de Hezbollah estuvo volando en espacio aéreo israelí entre 15 y 30 minutos. En 2006 las fuerzas israelíes derribaron tres UAV, uno de ellos cargado con 30 kilos de explosivos. En septiembre de 2014, Hezbollah mataba a 23 miembros del Frente al-Nusra (afiliado a Al-Qaeda) con un dron con carga explosiva o con un misil en Siria. Usos: vigilancia, comunicaciones externas y armado.
Hamas	Los primeros signos del programa de drones de Hamas son de 2003. En febrero de 2003, Hamas afirmaba que las fuerzas israelíes habían matado a seis de sus miembros mientras estaban montando un vehículo aéreo no tripulado. En 2005 los servicios de inteligencia israelíes desmantelaban una célula que estaba intentado transferir tecnología e información a Hamas desde una compañía en Emiratos Árabes. Probablemente Hamas se ha beneficiado de los UAS israelíes averiados, estrellados o derribados en territorio palestino desde mediados de 2000 en adelante. En el verano de 2014, Hamas lanzó como mínimo dos drones en Israel; uno de ellos supuestamente transportaba cuatro misiles tierra-aire. Usos: vigilancia, comunicaciones externas y supuesto armado.
Daesh	Daesh tiene un programa de drones institucionalizado, y lleva planeando su armado como mínimo desde 2015. Además, lleva tiempo adquiriendo hardware y otras herramientas para modificar y mejorar el rendimiento de drones comercialmente disponibles y para construir sus propios modelos inspirándose en otros preexistentes. Constituye un usuario muy prolífico de drones comerciales, además, creativo. En octubre de 2016, dos soldados kurdos resultaron muertos y dos miembros de las fuerzas especiales francesas fueron heridos por una bomba alojada en un dron de Daesh capturado por las fuerzas kurdas en Irak. La bomba explosionó mientras trasladaban el dron a la base para examinarlo. Usos: vigilancia, comunicaciones externas y armado.

Tabla 6. Ejemplos de actores no estatales que usan sistemas robóticos y autónomos. Fuente: Elaboración propia a partir de Bunker, 2015, pp. 13-15; Rassler, 2016, pp. 13-39; y Rassler et al., 2017.

Es necesario contar con una buena inteligencia y con conocimiento situacional sobre los actores no estatales violentos. Por un lado, eso incluye cuestiones como disponibilidad de recursos, tamaño y composición de la organización, y estrategia y tácticas de la entidad. Por el otro, hacen falta informaciones detalladas como la actitud de los líderes respecto a la innovación, la aversión al riesgo y/o a los fallos, y la experiencia técnica y de ingeniería específicas para completar labores complejas (Littlewood, 2016, p. iii).

El conocimiento situacional no solo debe servir para prever el éxito de las tareas de ingeniería compleja, sino también debe permitir contrarrestar las acciones y dificultar las labores a través de la identificación y la manipulación de cuellos de botella. Eso incluye la creación de obstáculos adicionales para los actores no estatales violentos

(recursos materiales, personal o riesgo de detección), y hacer que todo el entorno operativo sea más proclive a los fallos tácticos a la hora de conseguir armas (Littlewood, 2016, p. iii).

6. EN TODOS LOS DOMINIOS

La evaluación de los casos conocidos de empleo de sistemas no tripulados por actores no estatales como terroristas, insurgentes, criminales, corporaciones y activistas de todo el mundo permite identificar dos categorías principales de usos hostiles: ataques y recopilación de inteligencia (Open Briefing, 2016, p. 10).

Los usos hostiles y criminales de sistemas robóticos y autónomos por actores no estatales pueden suceder en todos los dominios. Sin embargo, el aéreo es el que más supuestos tiene documentados.

El motivo de que los UAS sean los más utilizados es la mayor variedad y cantidad de modelos comercialmente disponibles que además ofrecen más prestaciones que sus equivalentes terrestres y marítimos (Open Briefing, 2016, p. 10).

De la revisión de los usos históricos y contemporáneos y de las tentativas de uso en complots con sistemas aéreos no tripulados (UAS) por terroristas e insurgentes se pueden extraer las siguientes capacidades ya alcanzadas (Bunker, 2015, p. 16-19):

- Vigilancia y reconocimiento. La vigilancia en tiempo real es la menos común, pero puede servir para fines propagandísticos y para tareas de mando, control y coordinación.
- Mensajería. En varias formas, desde las más básicas de protesta, pasando por la propaganda interna o externa, hasta como advertencia a los adversarios de que la próxima vez se utilizará fuerza letal.
- Entrega de artefactos explosivos improvisados (IED). Equipar drones con IED para atacar diversos objetivos, desde personas relevantes a instalaciones emblemáticas o centros de mando y control.
- Entrega de armas de destrucción masiva. Potencialmente los drones pueden cargar y lanzar armas biológicas, químicas e incluso radioactivas.
- Plataforma armamentística. Se pueden instalar cohetes y misiles, pero también armas de fuego.

Aparte, es posible detectar otras capacidades actuales relativas a los sistemas aéreos no tripulados ligadas a otros actores que no son terroristas ni insurgentes, como las que aparecen a continuación (Bunker, 2015, pp. 19-21):

- Contrabando por crimen organizado y delincuentes (narcóticos, tabaco, y dispositivos móviles).
- Capacidades de inteligencia electrónica limitadas (hackear dispositivos móviles con fines de fraudes bancarios, robo de identidad o secuestro de personas).
- Aprovisionamiento logístico (alimentos y municiones).

- Rendirse a la fuerza opositora. A finales de febrero de 1991, durante la Primera Guerra del Golfo, se produjo la primera rendición conocida de un grupo de soldados ante un robot en un conflicto armado[3].

Recientemente, se recuperaba en Irak una veintena de documentos internos de Daesh sobre drones, fechados en 2015, proporcionados al Combating Terrorism Center (CTC) en West Point. Entre ellos hay unos formularios que muestran los tipos de misiones: avión explosivo; anti-dron; bombardeo; espionaje; entrenamiento; y pruebas (Rassler, a-Ubaydi y Mironova, 2017).

Por otro lado, el dominio acuático (marítimo y fluvial) es de especial interés por motivos de defensa y de seguridad interior, sobre todo en países como España, debido a su ubicación intercontinental. Las costas y las riberas de los ríos de nuestro país presentan una extensa superficie de ataque que actores malintencionados pueden explotar.

El conocimiento situacional del dominio marítimo en muelles y puertos y la protección de barcos y activos militares navales se han centrado en las amenazas a nivel de superficie de botes suicidas o entradas no autorizadas. Actores malintencionados pueden utilizar vehículos no tripulados de superficie (USV) y bajo superficie (UUV) para comprometer la seguridad de orillas y riberas. También se pueden producir ataques con vehículos aéreos no tripulados (UAV) contra USV y UUV. La detección de robots maliciosos y las estrategias para reducir el riesgo de un ataque exitoso no están explícitamente tratados en los procedimientos de conocimiento situacional del dominio marítimo (Patterson y Patterson, 2010, p. 1).

El personal de seguridad suele descartar las amenazas a la seguridad en orillas y riberas a nivel de superficie y bajo superficie por una serie de motivos:

1. Falta de inteligencia a corto plazo sobre actores que han estado trabajando con sistemas no tripulados.
2. Cálculos erróneos de que orillas y riberas no pueden ser destruidas usando capacidades de carga de sistemas no tripulados de bricolaje.
3. Necesidad de un disparo de precisión para hundir un objetivo reforzado como un buque de guerra moderno (Patterson y Patterson, 2010, pp. 1-2).

Todo esto supone ignorar el valor significativo de la guerra asimétrica para interrumpir la actividad de un puerto, incluyendo las pérdidas económicas que pueden alargarse indefinidamente (Patterson y Patterson, 2010, p. 2).

Tanto los vehículos no tripulados bajo superficie como los de superficie son instrumentos potenciales para los terroristas. Los UUV son técnicamente más complejos con respecto a la navegación y al tratamiento contra la presión del agua a gran profundidad, pero son mucho más furtivos. Los USV son más fáciles de detectar durante su aproximación pero todavía representan un riesgo considerable si se lanzan muchos durante un ataque de enjambre (Patterson y Patterson, 2010, p. 2).

3 Un reducido grupo de soldados iraquíes se rindió ante un dron Pioneer RZ-2A de Estados Unidos en la isla de Faylaka, cerca de la ciudad de Kuwait, para evitar enfrentarse a otro bombardeo del acorazado U.S.S. Missouri. El dron, que volaba bajo, funcionaba como observador transmitiendo vídeo en tiempo real para seleccionar objetivos y evaluar daños en el campo de batalla (Bunker, 2015, p. 21).

Entre los operadores de vehículos no tripulados sin propósitos terroristas figuran agencias hidrográficas, agencias de defensa, agencias de gestión de recursos e instituciones académicas. Aunque los vehículos submarinos están sujetos a controles de exportación, muchos de esos activos están mal custodiados por sus instituciones, y se pueden robar fácilmente (Patterson y Patterson, 2010, p. 2).

Todas las misiones con vehículos no tripulados tienen similitudes, incluyendo las realizadas por terroristas. Las etapas comunes son planificación, lanzamiento y supervisión de la misión. Una planificación adecuada incluye el análisis de información sobre batimetría, densidad del agua y corrientes, lo que incluye el estado de las mareas. Los sistemas de observación oceánica en tiempo real son de gran ayuda para planificar y completar misiones; reducen el riesgo de encallamiento y aumenta la eficiencia económica (Patterson y Patterson, 2010, p. 2). Ahora bien, esos sistemas están cada vez más disponibles para el público general a nivel mundial. Eso incluye a los actores maliciosos, que pueden aprovechar esa información para planear y ejecutar misiones hostiles y criminales.

Esos datos de sistemas de observación oceanográfica en tiempo real podrían servir para que, por ejemplo, un vehículo no tripulado pueda lastrarse correctamente a varios kilómetros del objetivo, con predicciones de tránsito muy precisas. Igualmente, el vehículo no tripulado puede conseguir datos de esos sistemas durante la ejecución de la misión, vía redes móviles e inalámbricas, por ejemplo, para realizar ajustes, redirigirse a un nuevo objetivo o abortar la misión (Patterson y Patterson, 2010, p. 2).

Los sistemas marítimos no tripulados son magníficas plataformas de inteligencia, vigilancia y reconocimiento (ISR) para actores malintencionados. Por ejemplo, pueden ser útiles para preparar un barco suicida o colocar explosivos con métodos más convencionales como un coche o un camión. Además, los datos de imágenes y sonar recopilados pueden servir para operaciones de guerra psicológica contra instalaciones marítimas (Patterson y Patterson, 2010, p. 3).

Las posibles cargas explosivas que un vehículo marítimo no tripulado puede transportar oscilan entre el tamaño de la bomba de un terrorista suicida (el equivalente a 9 kg de C-4) hasta el de un pequeño coche bomba (100 kg de C-4). Aunque esas plataformas no sean capaces hundir un buque de guerra moderno, pueden emplearse para atacar infraestructuras más vulnerables como oleoductos, muelles flotantes, barcos comerciales de cualquier tamaño, puertos y túneles de transporte que a menudo discurren bajo el agua en puntos de estrechamiento geográfico (Patterson y Patterson, 2010, p. 3).

Como los UMV suelen ser pequeños, pueden actuar en grupos reducidos, lo que supone una ventaja significativa de guerra asimétrica creando incertidumbre sobre lo que puede estar acechando ahí fuera. Un ataque con un solo robot contra una instalación costera o ribereña puede llevar a suponer que hay más cerca y que es inminente un nuevo ataque (Patterson y Patterson, 2010, p. 3).

Se espera una proliferación de sistemas no tripulados terrestres en los próximos años, debido a los avances en automóviles sin conductor. Probablemente con los coches autónomos suceda como con los UAV comerciales. Conforme se popularicen en el mercado, también quedarán al alcance de actores maliciosos. Entonces, será más difícil evitar su uso en atentados. Podrán pasar desapercibidos en carreteras, calles

y aparcamientos, en cualquier espacio donde un coche bomba podría causar daños considerables. Incluso si un coche autónomo está aproximándose o está aparcado cerca de una instalación gubernamental no hay ningún conductor al que los cuerpos y fuerzas de seguridad puedan indicar que lo mueva (Grossman, 2013, pp. 199).

Para aquellas organizaciones con presupuestos limitados y gran cantidad de personal, un vehículo bomba autónomo puede resultar menos rentable que sacrificar un terrorista suicida o un coche convencional de segunda mano. En cambio, para aquellos individuos y organizaciones con operativos valiosos, puede resultar interesante llenar un vehículo autónomo con explosivos. Un coche sin conductor con una bomba activada por teléfono móvil permite que un terrorista dirija el coche bomba al objetivo sin tener que visitar la escena antes de la explosión, evitando cámaras y posibles testigos. Si es un vehículo robado, o adquirido usando una identidad falsa, se complicará el rastreo del perpetrador (Grossman, 2013, pp. 198-199).

7. POSIBLES DESARROLLOS FUTUROS

Los robots pueden ser una tremenda fuerza para el bien, pero también pueden ser utilizados por delincuentes callejeros, acosadores, narcotraficantes y terroristas, una tendencia que seguramente se acelerará según sus funciones mejoren y sus precios bajen. Los mecanismos actuales de defensa y seguridad están pensados para proteger contra delincuentes humanos, no robóticos. Los drones pueden sortear cualquier valla, no solo las de las prisiones y las de las fronteras (Goodman, 2015, p. 313, 309).

En el futuro entorno operativo de 2035, algunos actores no estatales probablemente serán más influyentes que hoy en día. Los actores no estatales extremistas, a menudo motivados por cuestiones ideológicas y criminales, persistirán. En esa época, los extremistas serán capaces de explotar las tecnologías de la información y también pueden ser capaces de emplear una mayor variedad de capacidades militares (aunque a pequeña escala) usando tácticas innovadoras. Probablemente puedan desarrollar mayores niveles de letalidad para contrarrestar los sistemas de protección, e incluso pueden tener acceso a armas de efectos masivos. Las amenazas pueden abarcar desde ciberataques hasta vehículos aéreos no tripulados de actores no estatales hostiles que sobrevuelen una gran ciudad, quizás con un VIP como objetivo (Ministry of Defense UK, 2015, pp. 11-12, 42).

Las conexiones entre actores no estatales extremistas y las organizaciones criminales más poderosas probablemente se mantendrán. En los próximos veinte años, será más difícil distinguir entre criminales y terroristas. Además, aumentará la dificultad de diferenciar entre amenazas de Estados y de actores no estatales (Ministry of Defense UK, 2015, pp. 30, 40).

Los actores no estatales van a seguir utilizando UAV pequeños comercialmente disponibles para realizar diversos tipos de misiones. Es probable que sean principalmente labores de ISTAR (Inteligencia, vigilancia, adquisición de objetivos y reconocimiento), proporcionando obtención de inteligencia y capacidades de vigilancia que de otro modo serían difíciles o imposibles para tales grupos. Otras misiones que van a continuar siendo importantes son la adquisición de objetivos, la observación de artillería aérea, y la evaluación de daños en batalla. También es necesario destacar la importancia de los UAV en operaciones de información de actores no estatales;

a menudo su uso constituye una victoria propagandística para esos grupos (Friese, Jenzen-Jones y Smallwood, 2016, p. 58).

Según el mercado de drones comerciales continúe creciendo en todo el mundo, la competencia en el segmento comercial de gama alta probablemente se traduzca en mayores capacidades disponibles a menor precio, excluyendo los aspectos militares de esas capacidades, como los sistemas de vigilancia y de lanzamiento de armas más avanzados. Además, conforme los drones pasen de ser una capacidad de nicho a formar parte de cómo los ejércitos generan y despliegan la fuerza militar, sus efectos indudablemente cambiarán. Según la tecnología mejore, resultarán más accesibles para aquellos ejércitos sin un amplio apoyo logístico, e igualmente serán más útiles para militantes y activistas (Horowitz et al., 2016, p. 32-33)

Los actores no estatales podrían utilizar los drones pequeños como armas baratas y rudimentarias. Países como Estados Unidos suelen tener sofisticadas defensas aéreas centradas en objetos aéreos grandes, o defensas de tierra avanzadas equipadas para detener un camión lleno de explosivos, pero los actores no estatales podrían sembrar el caos con drones que sean el equivalente de bombas suicidas (Horowitz et al., 2016, p. 37).

Según los actores no estatales adquieran experiencia con los UAV, se prevén usos novedosos y técnicamente avanzados. La capacidad de esos grupos para armar UAV pequeños dependerá tanto del desarrollo de municiones equivalentes a los de las plataformas no tripuladas militares y policiales y de la proliferación de dichas armas, como del proceso de experimentación y de pruebas operativas de cargas ofensivas improvisadas por parte de los actores no estatales (Friese, Jenzen-Jones y Smallwood, 2016, p. 58).

Es posible proyectar varios escenarios de amenaza relativos al uso de UAV armados por actores no estatales (Friese et. al., 2016, p. 28-29):

1. El más común es su empleo para desplegar artefactos explosivos, ya sea un IED o una pieza de artillería convencional modificada, como una granada de mano o proyectiles de mortero. Pueden servir para ataques masivos e indiscriminados en zonas pobladas o para ataques de precisión donde un UAV puede penetrar un área segura. Dependiendo del tamaño y la capacidad del UAV y del método de integración de la carga, es posible transportar más de un artefacto explosivo. Cualquier carga desplegable también requeriría la inclusión de un mecanismo de lanzamiento manejado a distancia y respetar los requisitos específicos de armado y de iniciación de la carga ofensiva.

2. Otro es la utilización de un UAV pequeño como IED aéreo, con los explosivos incorporados al propio aparato, que actúa como mecanismo de distribución. Esto necesitaría un sistema de iniciación, probablemente un detonador con retardo, un detonador de impacto en el morro de la aeronave, un detonador activado mediante comandos o una combinación de los anteriores. Según el componente explosivo utilizado, incluso una pequeña cantidad de explosivo potente podría resultar destructiva contra objetivos no blindados como personas, automóviles, edificios o infraestructuras críticas.

3. Una posibilidad menos probable es el montaje de armas ligeras, como una pistola, por la dificultad de mantener un UAV en una posición fija. La eficacia de esta aplicación es cuestionable, porque incluso el retroceso de un arma de fuego ligera

afecta dramáticamente a la estabilidad de un UAV pequeño y a la precisión de disparo. Sin embargo, los UAV con mayor peso al despegue bruto podrían verse menos afectados por el efecto de retroceso (Friese et. al., 2016, p. 28):

4. Las cargas químicas o biológicas dispersadas desde un UAV podrían resultar devastadoras contra objetivos en exteriores, como aglomeraciones de público o embalses de agua. La potencia de tales ataques depende casi completamente de la carga específica, pero incluso una poco eficaz podría tener un impacto simbólico o psicológico sustancial. Algunas tecnologías civiles y policiales actualmente en desarrollo, como las armas menos letales y los drones fumigadores, podrían ser adaptadas para la distribución de agentes biológicos o químicos.

5. Aunque no sean considerados armas convencionales, ciertos dispositivos de radiofrecuencias se pueden emplear con fines ofensivos. Las cargas diseñadas para penetrar redes inalámbricas con propósitos de vigilancia o ciberataque están disponibles. Lo mismo sucede con las radios tradicionales y el software para hackear radiofrecuencias, que podrían utilizarse para interferir señales de navegación aérea, policiales y de servicios de emergencia, así como otras redes inalámbricas.

6. El propio UAV sin armar puede representar una amenaza en un ataque de golpe de pájaro, introduciéndose intencionadamente en el motor de un avión de pasajeros. Asimismo, dejar caer cualquier peso inerte puede resultar peligroso. En acontecimientos al aire libre con multitud de personas, arrojar líquidos o cualquier objeto desde un pequeño UAV puede provocar pánico en masa. Eso puede acabar causando bajas directamente, o funcionar como distracción en ataques coordinados y complejos (Friese et. al., 2016, p. 29).

Algunos de los escenarios más inquietantes están relacionados con la tecnología autónoma no retirable[4], ideada para asegurar un nuevo tipo de destrucción mutua autónoma, y que es aplicable a los sistemas no tripulados y al software de control de armas.

La mayoría de los fundamentos técnicos necesarios para la tecnología autónoma no retirable ya existen, pero unos pocos elementos esenciales todavía no están completamente desarrollados. Está definida por cuatro aspectos (Straub, 2016, p. 42):

1. La tecnología puede recibir órdenes para atacar a un grupo particular o a una clase de objetivos;

2. es capaz de localizar miembros de ese grupo o clase y de evaluar si un objetivo potencial pertenece a ese grupo o clase;

3. puede atacar un objetivo seleccionado; y

4. esas órdenes, una vez dadas, no se pueden revocar.

El sistema además puede incorporar elementos adicionales, como la habilidad de adaptarse a condiciones cambiantes, buscar refugio, defenderse a sí mismo y recopilar todo lo que necesite (Straub, 2016, p. 42).

4 La noción de no retirable en el contexto de la inteligencia artificial implica que se le encarga una tarea que no se puede anular. La inteligencia artificial seguirá intentando cumplir la misión hasta que lo consiga o hasta que reciba daños que impidan completarla, total o parcialmente (Straub, 2016, p. 43).

El principal problema de la tecnología autónoma no retirable es que la situación puede cambiar haciendo irrelevantes la órdenes iniciales en el contexto actual, por ejemplo, si un adversario quiere rendirse. Es posible plantear varios escenarios donde un actor no estatal puede hacer uso de sistemas autónomos no retirables. Puede ser el caso de uno que tema ser destruido pero que quiera conseguir concesiones políticas de un Estado. Puede ser incluso un recurso más efectivo en situaciones donde el actor no estatal emplea la amenaza de utilizarlo para proteger a sus bases, en lugar de plantear demandas (Straub, 2016, pp. 44-45).

La creación de drones autónomos y no retirables conforma escenarios similares a la Guerra Fría. Quizás continúe siendo un terreno donde nadie se atreva a dar el primer paso. Limitaciones tecnológicas (especialmente las relacionadas con la selección autónoma de objetivos) impedirán recorrer ese camino durante un tiempo, pero probablemente se superarán. Los Estados pueden ser más reacios (al menos públicamente) a adoptar o defender el uso de este tipo de tecnología. Sin embargo, basta con que un único actor con alta capacidad técnica inicie la cadena de acontecimientos. Y los actores no estatales con poco que perder presentan la mayor amenaza (Straub, 2016, p. 46).

8. CONCLUSIONES

El interés de los actores no estatales por los sistemas robóticos y autónomos (RAS) se remonta a más de veinte años. Los usos hostiles de esos sistemas están protagonizados por una gran variedad de actores (colectivos e individuales), motivados por muy diversas ideologías.

Los RAS ponen en manos de todo tipo de grupos e individuos capacidades que antes estaban reservadas a las fuerzas armadas. En los últimos años, se han reducido las barreras de entrada para acceder a sistemas no tripulados debido a la creciente oferta comercialmente disponible. De hecho, los actores no estatales tienen varios métodos para conseguirlos: adquirirlos, modificarlos, construirlos o hackearlos.

Los sistemas no tripulados resultan atractivos por los beneficios y capacidades que proporcionan. Hacen más fácil, más seguro y más barato que personas no expertas adopten nuevas tácticas y armas, incluyendo las de destrucción masiva.

Cuando las condiciones son adecuadas, casi cualquier tarea técnica, incluso las más complejas, son factibles para los actores no estatales violentos. Algunos ejemplos de actores no estatales que desarrollan programas estables de sistemas robóticos y autónomos son Hezbollah (como mínimo desde 1997), Hamas (desde 2003) o Daesh (mínimo desde 2015).

En este siglo XXI la influencia sistémica de los actores no estatales violentos va a crecer, una dinámica que puede verse exacerbada por la difusión de tecnologías emergentes en la sociedad. En concreto, existe la preocupación de que los actores no estatales adopten tecnologías emergentes, como los sistemas robóticos y autónomos, para aumentar la amenaza que presentan para la seguridad internacional.

En general, los vehículos aéreos no tripulados [los más utilizados de todos los sistemas robóticos y autónomos] son viables y potencialmente efectivos en diversos tipos de ataques. Sin embargo, a menudo no suelen resultar más ventajosos que otras alternativas de llevar a cabo operaciones contra objetivos similares. Así, los UAV representan una ‘amenaza de nicho’, con ciertas contribuciones potenciales a la amenaza terrorista y asimétrica, más que constituir un modo de ataque

ampliamente adoptado por tales actores (Jackson, Frelinger, Lostumbo y Button, 2008, p. 58).

El empleo de drones por terroristas supone una amenaza de nicho que sigue siendo baja. Los resultados de éxito han sido la excepción, no la regla. Sobre todo se utilizan con fines de vigilancia y de comunicación estratégica, para publicitar su habilidad de penetrar áreas negadas, para recopilar inteligencia o para provocar miedo entre sus adversarios (Rassler, 2016, p. 47).

La amenaza actual de una entidad terrorista usando un solo UAS (sistema aéreo no tripulado) controlado a distancia es de moderada probabilidad y con consecuencias de letalidad entre bajas y moderadas. Aunque cualquier futuro ataque terrorista con un UAS sea novedoso y digno de atención, y ayude al grupo a ganar notoriedad, tal ataque es poco probable que sea estratégico, excepto en los siguientes supuestos:

- Sirva para ejecutar el asesinato selectivo de una personalidad importante bien protegida;
- mate a personas dentro de un área fuertemente protegida, como la Casa Blanca o el Centro de Investigación Nuclear Negev en Israel;
- disperse eficazmente armas químicas, biológicas o radiológicas; o
- use el UAS de una manera que cause mucha conmoción, esté bien publicitada o sea creativa, o quizás esté combinada con otros sistemas de armas en un entorno urbano o en un acontecimiento muy concurrido, de forma que la ingenuidad del propio ataque lo convierta en estratégico (Rassler, 2016, p. 48).

La cantidad y la sofisticación de los sistemas no tripulados probablemente también aumentará el alcance y la gravedad de la amenaza, y afectará a las consecuencias de futuros incidentes. Por ejemplo, un ataque con UAS utilizando un grupo de drones o un enjambre que funcione cooperativamente y con autonomía tiene el potencial de aumentar la letalidad del ataque antes y después, así como su impacto psicológico y su complejidad. Las principales variables que amplifican el potencial estratégico de un complot terrorista con UAS proceden de los beneficios únicos que los drones proporcionan, como la intimidad y la facilidad de acercarse a los objetivos (Rassler, 2016, p. 48).

El peligro inmediato del uso de sistemas no tripulados por actores terroristas es la formación de equipos de humano-máquina. Las tecnologías están trasladando la fuerza desde el poder duro y las armas convencionales a las soluciones ‘artísticas’ que involucran el uso combinado de elementos pequeños, rápidos y en grandes números (Rassler, 2016, p. 62). En ese aspecto reside el futuro de los sistemas robóticos y autónomos como tecnología emergente con potencial disruptivo.

En definitiva, los usos hostiles de sistemas robóticos y autónomos por parte de actores no estatales, ya sean grupos o individuos, representan desafíos a la seguridad y la defensa nada despreciables. Pueden llegar a suponer un gran desgaste para los Estados, por las capacidades asimétricas que facilitan y por los altos costes de las contramedidas.

REFERENCIAS BIBLIOGRÁFICAS

Ackerman, G. A. (2016a). "Designing Danger": Complex Engineering by Violent Non-State Actors: Introduction to the Special Issue. *Journal of Strategic Security, 9*(1), 1-11.

Ackerman, G. A. (2016b). Comparative Analysis of VNSA Complex Engineering Efforts. *Journal of Strategic Security, 9*(1), 119-133.

Bunker, R. J. (2015). *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications*. Carlisle Barracks: United States Army War College Press.

Clapham, A. (2016, 19 diciembre). "Non-State Actors". Recuperado de https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1626284&v=1392752313000

Cockburn, A. (2015). *Kill Chain: The Rise of The High-Tech Assassins*. Nueva York: Henry Holt and Company.

Eliasson, J. (2016, 15 diciembre). Deputy Secretary-General's remarks to the Security Council on Proliferation of Weapons of Mass Destruction by Non-State Actors [as prepared for delivery]. Recuperado de https://www.un.org/sg/en/content/dsg/statement/2016-12-15/deputy-secretary-generals-remarks-security-council-proliferation

Friese, L., Jenzen-Jones, N. R. y Smallwood, M. (2016, febrero). *Emerging Unmanned Threats: The use of commercially-available UAVs by armed non-state actors*. Perth, Australia: ARES (Armament Research Services).

Gartenstein-Ross, D. (2014). Violent Non-State Actors: Paradigmatic Lessons Learned. En CPPR-Centre for Strategic Studies, *National Security Management in Federal Structures: Perspectives from India and the United States* (pp. 48-57). Kochi: Centre for Public Policy Research.

Gartenstein-Ross, D. y Zenn, J. (2017, 16 enero). *Terrorists, Insurgents, Something Else? Clarifying And Classifying The "Generational Challenge"*. Recuperado de http://fortunascorner.com/2017/01/16/terrorists-insurgents-something-else-clarifying-and-classifying-the-generational-challenge/

Goodman, M. (2015). *Future Crimes: A Journey to the Dark Side of Technology - and How to Survive it*. Londres: Transworld Publishers.

Grossman, N. (2013). Robotics and The Future of International Asymmetric Warfare [Tesis doctoral].

Horowitz, M. C., Kreps, S. E., Fuhrmann, M. (2016, 25 enero). *The Consequences of Drone Proliferation: Separating Fact from Fiction*. International Security (en prensa).

Jackson, B. A., Frelinger, D. R., Lostumbo, M. J., y Button, R. W. (2008). *Evaluating Novel Threats to Homeland: Unmanned Aerial Vehicles and Cruise Missiles*. Santa Monica, California: RAND.

Kyriakopoulos, G. D. (2016). Formation of International Custom and the Role of Non-State Actors. En Pazartzis, P. y Gavouneli, M. (Eds), *Reconceptualising the Rule of Law in Global Governance, Resources, Investment and Trade* (pp. 43-58). Portland, Oregon: Hart Publishing.

Laborie Iglesias, M. A. (2011). Actores armados no estatales y modelo de Estado. En IEEE, *Cuaderno de Estrategia nº 152: Actores armados no estatales: retos a la seguridad global* (pp. 27-64). Ministerio de Defensa de España.

Littlewood, J. (2016). Foreword to Special Issue on Complex Engineering by Violent Non-State Actors. *Journal of Strategic Security, 9*(1), i-iii.

Ministry of Defense UK. (2015). *Strategic Trends Programme: Future Operating Environment 2035*.

Open Briefing. (2016, enero). *Hostile Drones*. Londres: Remote Control Project.

Patterson, M. R. y Patterson, S. J. (2010). *Unmanned Systems: an Emerging Threat to Waterside Security: Bad robots are coming*. Waterside Security Conference (WSS) 2010. doi: 10.1109/WSSC.2010.5730271

Rassler, D. (2016, octubre). *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology*. West Point: Combating Terrorism Center, U.S. Military Academy.

Rassler, D., al-Ubaydi, M. y Mironova. V. (2017, 31 enero). The Islamic State's Drone Documents: Management, Acquisition, and DIY Tradecraft. CTC Perspectives. Recuperado de https://www.ctc.usma.edu/posts/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft

Straub, J. (2016). Consideration of the use of autonomous, non-recallable unmanned vehicles and programs as a deterrent or threat by state actors and others. *Technology in Society, 44*, 39-47.

United Nations, Security Council. Resolution 2325 (2016), Adopted by the Security Council at its 7837th meeting, on 15 December 2016. United Nations S/RES/2325 (2016). (Diciembre 15, 2016)

US Army. (2016, septiembre 30). *The US Army Robotic and Autonomous Systems Strategy*.

World Economic Forum. (2016). *Global Risk Report 2017 - 12th Edition*.

Yin, T. (2015) Game of Drones: Defending Against Drone Terrorism. *Texas A&M Law Review(3)*, 4, 634-673.

Fecha de recepción: 04/04/2017. Fecha de aceptación: 30/06/2017