# Inteligencia Artificial en Small - Unmanned Aircraft System (S-UAS) como amenaza cibernética



Mayor Iván Darío Cárdenas Rodríguez

Alumno CEM 2023

Magíster Ciberseguridad y Ciberdefensa

TC Milena Elizabeth Realpe Díaz

Curso de Estado Mayor CEM

Contexto en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Bogotá

2023

## Resumen

Los avances de la tecnología y su rol en diferentes áreas de la cotidianidad, así como áreas industriales e incluso del sector defensa son cada vez más sorprendentes. El presente documento aborda el desarrollo de los S-UAS (Small – Unmanned Aircraft System) y su relación con otras tecnologías disruptivas, planteando principalmente desde la inteligencia artificial cuáles son sus alcances y hasta donde la humanidad y las sociedades podrían permitir un incremento sin fin de estas capacidades de aprendizaje de las maquinas, que incluso podrían sobre pasar las capacidades del hombre como especie.

Posterior, se presenta una categorización de la AI según sus niveles de complejidad en las decisiones programadas, y como estas pueden direccionar sus capacidades hacia una Zona Gris donde se pierda el control y trazabilidad de lo que podrían llegar a hacer estas plataformas.

Del mismo modo, se plantea la necesidad de contar con una contramedida disruptiva para el control de estos sistemas desde la cibernética, que evite las características de las contramedidas actuales las cuales generan efectos no deseados cuando se trata de ambientes aeronáuticos o de infraestructura crítica.

# Inteligencia Artificial en Small - Unmanned Aircraft System (S-UAS) como amenaza cibernética

El imparable avance de la tecnología, cada vez más embebida en la sociedad y transversal ahora a todas las dimensiones de la vida diaria, han llevado a que esta sea parte esencial, y normal, de la manera en la que como individuos y como sociedad, llevamos a cabo tareas y misiones en gran cantidad de campos, comerciales, científicos, deportivos e incluso militares y a su vez satisfacemos necesidades haciendo uso de herramientas tecnológicas inteligentes.

Dichas herramientas avanzan a gran velocidad con un objetivo claro, reducir la intervención del hombre tanto en su operación como en sus procesos lógicos, aplicando capacidades para aprender de manera perenne (Machine learning) e incluso tomar decisiones basadas en la manera como interpretan la información que capturan de su entorno, tanto físico como cibernético (Artificial Inteligence), es ahí donde este documento plantea: para el caso puntual de los S-UAS ¿Es la Inteligencia Artificial aplicada a los S-UAS un avance, o una amenaza?

 El desarrollo de esta tecnología ha sido imparable y vertiginoso en las últimas 3 décadas. Estas plataformas aéreas, encajan de manera perfecta en la categoría de tecnología disruptiva pues son innegables sus capacidades, las cuales se encuentran en constante crecimiento y desarrollo, con un costo en todos los aspectos mucho menor que una aeronave tripulada y en la mayoría de los casos con mayor eficiencia (CITAR).

Refencia de la imagen.

En el contexto de las sociedades con economías en desarrollo, es aún determinante el apego a conceptos establecidos, incluso siendo aún arcaicos, los cuales limitan la posibilidad de maniobra o modificación de estructuras sociales, de conocimiento o de pensamiento. Esta condición lleva a que a pesar que el mundo se haya desplazado hacia ejes distintos, sigamos de muchas maneras apegados al pasado, objetando los retos y los riesgos que cierne sobre nosotros todos aquellos tráficos de información que transitan por el ciberespacio, ralentizando el diseño y creación de medidas eficientes y efectivas de ciberseguridad y ciberdefensa (citar) que hagan una defensa contra los drones comerciales o S-UAS por su sigla en inglés (Small – Unmanned Aircraft System). En contraste, aquellos agentes interesados en desestabilizar un país, un sistema de gobierno, un sistema económico, y en general el orden mundial avanzan sin descanso inventando y reinventando amenazas dos o tres pasos por delante de nosotros.

## **Inteligencia, o Amenaza Artificial?**

La revolución industrial trajo consigo grandes avances para la humanidad, las maquinas son ahora capaces de replicar actividades realizadas por el hombre de manera autónoma con una intervención mínima o nula de sus operadores para cumplir tareas para las cuales antes se requería de manera intensiva la mano de obra. Este concepto de automatización ha sido objeto de desarrollo y perfeccionamiento continuo, hemos llegado al punto de tener máquinas capaces de tomar decisiones y ofrecer a su usuario los mejores y más objetivos cursos de acción de acuerdo con su programación, haciendo cada vez más sencillo y rápido el proceso de la toma de decisiones en un amplio abanico de escenarios, que pueden ir desde tareas triviales, como la hora en la que programamos electrodomésticos para que se enciendan y se apaguen, hasta los cursos de acción críticos como cuando una sistema de armamento deba rastrear, enganchar y destruir un blanco mediante el empleo de armamento estratégico de destrucción masiva.

Ese planteamiento ha sido explorado y categorizado por Paul Scharre, oficial retirado del Ejército de los Estados Unidos y experto en defensa del Pentágono quien pone sobre la mesa la discusión de lo que implicaría permitir que las máquinas, dentro del círculo de decisión programado para enganchar y batir un objetivo, tengan la decisión final sobre la vida o la muerte de una persona. Por tal motivo, se puede inferir que bajo la luz de la ética, los sistemas de armas más sofisticados en su matriz y algoritmos de decisión, siempre deben tener activa la relación entre la maquina y el hombre, la cual establezca que la decisión final siempre estará a cargo del operador, nunca en modo autónomo.(CITAR) Este autor define tres categorías, en primer término las clasifica de acuerdo con el nivel de criticidad de las tareas y decisiones que la maquina debe cumplir. En segundo lugar, cuales son las consecuencias de las decisiones que tome la maquina en caso de que la misma falle. Si a esto, se le suma que las maquinas ahora actúan dentro de un ecosistema dentro del cual aprenden de manera constante y con mas precisión incluso que sus creadores, es posible llegar a enfrentar escenarios donde las maquinas según su criterio objetivo, vean comprometida su integridad y busquen el dominio y supremacía de sus acciones por encima de sus operadores o creadores. En tercer lugar, la sofisticación de la decisión de la máquina al cumplir la tarea.

Es importante tener en cuenta que este tipo de tecnologías, así como las demás categorías clasificadas como disruptivas,(citar) todas actúan y se relacionan entre sí formando un ecosistema, es decir que en algún momento se favorecen o aprovechan los productos de otras para su propio desarrollo y también entregan productos a los demás componentes. Al respecto, los drones no son la excepción, y a través de sus sensores y la interpretación de la información que reciben del mundo a través de estos son capaces de analizar su entorno, tal cual o incluso mejor que un humano para comprenderlo, interpretarlo, analizarlo y aprender de este. Es así como un drone programado correctamente y con los equipos adecuados, es capaz de convertirse en una amenaza para la seguridad, no solo física como ya ha sido ampliamente evidenciado y donde ya existen avances al respecto, sino también de generar ataques cibernéticos capaces de ingresar o suplantar redes para robar información o infligir daños en los sistemas a través de las redes empleando principios de la técnica conocida como SPOOFING, que consiste en engañar o suplantar la identidad de los usuarios para obtener de manera ilegal información.

La gran capacidad de adaptación y aprendizaje, mediante su relación y conexión por medio del IoT (Internet of Things), acceso a bases Big Data y la minería de datos entre otros, permiten predecir que las maquinas tendrán comportamientos con capacidad de adaptación a su entorno tal como lo haría un humano, por lo tanto, es inquietante el panorama del grado de autonomía que pueden llegar a adquirir si continua esta senda perpetua de desarrollo tecnológico.

Llegamos así, a identificar una posible Zona Gris (CITAR) en cuanto al uso hostil de este tipo de plataformas, las cuales no son exclusivamente aéreas, sino también terrestres, subterráneas, marítimas e incluso en el espació. Este último escenario, aunque no con intenciones hostiles, está siendo puesto en evidencia con el drone INGENUITY, desarrollado por la NASA para su última misión de exploración de marte, el cual funciona de manera completamente autónoma, tanto en sus sistemas de operación como en el procesamiento de datos de su entorno.

Esta Zona Gris para ciberataques con drones, cumple con los criterios de ser actividades hostiles y de difícil detección en el ciberespacio (CITAR), nos plantea un potencial bélico no cinético que puede incidir negativamente en la seguridad de activos estratégicos de una nación. Al respecto, se encuentra completamente relevante el concepto de seguridad integral, donde no solo se encuentre componente físico, sino también el espacial y ciberespacial, entendiendo que es menester sobrepasar los conceptos tradicionales y estáticos, con dirección a medidas que tengan la capacidad de aprender y adaptarse a su entorno, pues los mismos no actúan en un solo dominio, sino también pueden construir una relación simbiótica con sistemas más tradicionales, por ejemplo un SOC (Security Operations Center) que pueda integrar de manera activa las barreras físicas y sensores de video con acceso a Big Data e IoT, interconectados con otros organismos de seguridad para un control y seguimiento detallado de cada individuo que ingrese a una instalación.

Los antecedentes mundiales y locales, dejan en evidencia la intención de actores hostiles de emplear este tipo de plataformas autónomas o remotamente tripuladas, para perpetrar actos terroristas y de desestabilización. A nivel mundial, fue sorprendente la manera como un enjambre de S-UAS logro sobrepasar las defensas antiaéreas que protegían la refinería ARAMCO en Arabia Saudi, las más grande del mundo, paralizándola y dejando al desnudo sus vulnerabilidades ante este tipo de sistemas que hasta ese momento habían sido subestimados, pero sobre todo dejando en evidencia que no hay límites para este tipo de plataformas.

La disponibilidad de componentes para construir y potencializar las capacidades de estas plataformas, es cada día de más fácil acceso. Los desarrollos tanto en equipos como en formación de personal especializado, han hecho que construir un Drone simple con capacidades que comprenden rangos de hasta 15 km, autonomías superiores a 40 minutos y capacidades de carga para de más de 500 gramos sea cada vez más fácil y barato, tal vez demasiado para personas o grupos con intenciones terroristas, lo que hace imprescindible actuar no solo tecnológicamente, sino políticamente para contener los alcances de las capacidades de equipos de venta libre y masiva. Al respecto se ha visto como ya Estados Unidos, restringe y controla la venta de equipos DJI de origen chino por los riesgos y brechas de seguridad que aseguran haber detectado en dichas maquinas las cuales supuestamente hacen el tránsito de datos por servidores bajo el control del gobierno del país asiático, y su información o incluso las mismas plataformas pueden ser utilizadas en contra del país y sus intereses.

# Conclusiones

Aunque desde 2019 se encuentra en desarrollo la capacidad para detectar e inhibir los S-UAS como amenaza y riesgo en las Unidades Militares de la FAC, es innegable que la oferta mundial es aún reducida, y con limitaciones y efectos colaterales que ponen en duda su eficiencia en este tipo de escenarios, en los cuales no solo es relevante la seguridad física de personal, material e instalaciones, sino también la seguridad operacional de las aeronaves pues la inhibición es aún un componente en desarrollo, y su principio de operación de alguna manera rudimentario a pesar de su avanzado estado, pues no es capaz de discriminar y enganchar el canal de comunicación entre el operador y la plataforma, es decir, no se adapta a la amenaza.

Es evidente, que las medidas cinéticas contra este tipo de elementos siempre generan efectos no deseados, ya sea por el ambiente en que se presentan hechos con drones, o por la dificultad de contrarrestar de manera efectiva un evento con múltiples drones desde diferentes cuadrantes. Es decir que su velocidad de desarrollo de las contramedidas, es considerablemente menor a la de la amenaza y especialmente débil, sin haber llegado aún a una solución disruptiva al respecto, es decir, que con un costo bajo, permita tener una mayor rendimiento en los resultados esperados.

Es necesario entonces, lograr una combinación efectiva de medidas, dando prioridad a las No cinéticas sobre las cinéticas, que tengan un alcance desde su fabricación hasta el usuario final y en lo posible un modo de trazabilidad en tiempo real, y que conlleve una configuración de permisos sobre la capacidad de las plataformas, de moto tal que no puedan, o por lo menos se limite la posibilidad de darle un uso irresponsable u hostil, así como permitir la fácil y rápida identificación tanto del equipo como del usuario que pretenda o se encuentre afectando la continuidad operacional de un aeródromo o cualquier infraestructura critica, como las bases aéreas o puestos militares.

Debemos entonces analizar si nuestros sistemas de seguridad están acordes a las nuevas amenazas, o si por el contrario nos atascamos en la guerra de trincheras y seguimos enredados entre la concertina de los modelos anacrónicos de seguridad.

Finalmente, es imprescindible limitar las capacidades de Inteligencia Artificial con las que se encuentran configurados estas plataformas, por lo menos en el caso de aquellas que son de libre distribución y adquisición, pues en el caso de sistemas que sean weaponizados (Armados) por el usuario final, estos podrían llegar a determinar de manera autónoma lo que representa un blanco legitimo o no de una manera tan objetiva que trasgreda las esferas éticas de la deshumanización de la guerra.

Así mismo, no se deben perder de enfoque otros aspectos de control, tales como el establecimiento de consensos y acuerdos para el desarrollo de una doctrina conjunta, que contemple de manera realista este tipo de elementos como una amenaza tangible, y que seguramente desde las áreas de ciberseguridad y ciberdefensa logremos encontrar el punto de quiebre que nos lleve al desarrollo de una tecnología disruptiva contra drones u otro tipo de vehículos autónomos eficiente y de bajo costo. Evidentemente, esto debe estar acompasado con desarrollos estructurales en los campos de capacitación de recurso humano al respecto, desarrollo doctrinal y regulatorio nacional e incluso internacional bajo el entendido que este tipo de plataformas, así como tienen grandes capacidades que han facilitado trabajos que antes requerirían gran cantidad de recursos económicos y humanos, tales como la topografía, la agricultura, búsqueda y rescate, la cartografía, la inspección de áreas críticas de difícil acceso, también en las manos equivocadas representan una amenaza con alcances globales.