MINISTERIO DE DEFENSA

ESTADO MAYOR DE LA DEFENSA

CONCEPTO NACIONAL C-UAS LSS

COUNTER UNMANNED AERIAL SYSTEMS LOW SLOW SMALL

CENTRO CONJUNTO DE DESARROLLO DE CONCEPTOS
CESEDEN
Paseo de la Castellana 61, Madrid

ENERO DE 2019

[REVERSO PORTADA]

Jefe de Estado Mayor de la Defensa

CARTA DE PROMULGACIÓN

En uso de las atribuciones que me otorga la Ley Orgánica 05/2005 de la Defensa nacional, apruebo en las Fuerzas Armadas el Concepto Nacional C-UAS LSS "Contra sistemas aéreos no tripulados de pequeño tamaño, que operan a baja altura y velocidad".

El presente Concepto deberá servir de guía y orientación para el correcto desarrollo de la capacidad de defensa C-UAS LSS, y su correspondiente Plan de Implementación.

El Concepto C-UAS LSS es un documento de USO PÚBLICO.

Madrid, a 23 de enero de 2019

El General de Ejército
Jefe de Estado Mayor de la Defensa

ESTADO MAYOR DE LA DEFENSA
JEFE

- Fernando Alejandre Martínez -

[INTENCIONADAMENTE EN BLANCO]

PREFACIO

En el último lustro, hemos sido testigos de un aumento exponencial del número de sistemas aéreos no tripulados (*Unmanned Aerial Systems*, UAS), conocidos popularmente como drones, empleados para fines muy diversos por parte de diferentes actores.

La proliferación casi sin control de los UAS de pequeño tamaño, pero grandes capacidades al alcance de cualquier usuario gracias a la gran oferta en el mercado, su bajo coste y la facilidad de manejo, ha ocasionado accidentes y situaciones potencialmente peligrosas debido al uso imprudente de los mismos.

Asimismo, actores estatales y no estatales han sabido aprovechar esta tecnología para emplearla con fines hostiles o maliciosos, ampliando su uso convencional en misiones de inteligencia, vigilancia, adquisición de blancos y reconocimiento, al empleo como vectores de ataque portando armas, municiones, explosivos, etc.

Estos UAS de pequeño tamaño, que vuelan a baja altura y velocidad (*Low Slow Small*, LSS), son difíciles de detectar, identificar y neutralizar por los medios actuales de Defensa Aérea basados o no en superficie. Por lo tanto, suponen una nueva amenaza para la seguridad de nuestras Fuerzas Armadas (FAS), tanto desplegadas en misiones en el exterior como en territorio nacional, así como para el resto de los ciudadanos.

Nos hallamos ante una amenaza creciente para la seguridad, que supone un reto tanto tecnológico como institucional para disponer de sistemas Contra UAS (C-UAS) LSS, capaces de evolucionar y adaptarse al ritmo que lo hacen las tecnologías y la propia amenaza, y que puedan hacerle frente de manera eficaz.

En este contexto, y conforme a la Directiva de desarrollo conceptual 01/2018 del JEMAD, el Centro Conjunto de Desarrollo de Conceptos ha liderado los trabajos de un grupo de expertos provenientes del ámbito del Ministerio de Defensa, el Ministerio del Interior, la Industria y la Academia, para elaborar un Concepto que oriente el desarrollo de una capacidad integral de Defensa C-UAS LSS, para garantizar la protección y libertad de acción de las FAS en los diferentes escenarios y entornos de actuación presentes y futuros.

A los efectos de este concepto, la categorización de la amenaza UAS LSS se centra en aquellos sistemas que debido a sus características, hacen que se sitúen fuera de la envolvente de detección, seguimiento, identificación y neutralización de los medios actuales de Defensa Aérea.

El Concepto C-UAS LSS está alineado y es compatible con las distintas iniciativas que actualmente se están desarrollando, tanto en el ámbito nacional (Proyecto CONDOR, Grupo interministerial de Drones*)* como en el internacional, particularmente en la OTAN y en la UE.

[INTENCIONADAMENTE EN BLANCO]

CONTENIDO

ANEXOS.

[INTENCIONADAMENTE EN BLANCO]

1. ANTECEDENTES.

01. A finales de diciembre de 2017, la Célula Nacional Contra IED (CENCIED) identificó y presentó una **propuesta de Problema Militar Operativo** (PMO) sobre el empleo de sistemas aéreos no tripulados utilizados como dispositivos armados improvisados: "*Las Fuerzas Armadas no cuentan con un conjunto de capacidades, ni procedimientos estandarizados que permitan a sus unidades e instalaciones detectar, identificar y derrotar la amenaza que supone el empleo de UAS (Unmanned Aerial Systems) LSS (Low, Slow, Small*) *como IWD (Improvised Weapon Devices)*".

02. La validación del PMO significó el reconocimiento no solo de la **carencia** de esta capacidad en las FAS españolas, sino también de la **necesidad** de introducirlo dentro del proceso de Planeamiento de la Defensa con el fin de desarrollar la capacidad C-UAS LSS.

03. Mediante Oficio GABTEC JEMAD S-18-000450, de 12/03/2018, se asignó al Centro Conjunto de Desarrollo de Conceptos (CCDC) la tarea de liderar el desarrollo del **Concepto "Contra Sistemas Aéreos No tripulados" (C-UAS)**, conforme a la visión y orientaciones incluidas en la Directiva de Desarrollo Conceptual 01/2018 del JEMAD (DDC 01/2018).

04. La DDC 01/2018 establece que los trabajos se realizarán de forma colaborativa entre expertos de todos los organismos involucrados, al objeto de alcanzar la **solución más eficaz** para nuestras FAS; el desarrollo del concepto está considerado como **urgente**, por lo que será elevado para la aprobación del JEMAD no más tarde del 15 de enero de 2019.

05. Paralelamente a este desarrollo conceptual, la Dirección General de Armamento y Material (DGAM) lanzó en el año 2018 el **proyecto CONDOR**, como una iniciativa de I+D+i "dirigida fundamentalmente a empresas de ámbito nacional, "*con objeto de realizar inicialmente una selección de aquellos sistemas maduros que, mediante un proceso de desarrollo posterior que complete sus capacidades desde el punto de vista militar, puedan dar respuesta a las necesidades de sistemas contra-dron que existen en las FAS*."

2. OBJETO.

06. El objeto del concepto C-UAS LSS es **orientar el desarrollo de la futura capacidad integral** que permitirá prevenir, detectar, identificar, decidir y, en su caso, neutralizar la amenaza de UAS LSS empleados de forma hostil o imprudente, contra unidades desplegadas en operaciones e instalaciones militares, dentro y fuera del territorio nacional.

3. ALCANCE.

07. A lo largo del desarrollo del concepto se plantean una serie de cuestiones e hipótesis en los diferentes elementos fundamentales identificados en la fase de investigación, que han sido analizadas, discutidas y desarrolladas por el Grupo de Expertos, para garantizar su validez en términos de **propiedad, aceptabilidad y practicabilidad**.

08. Partiendo del análisis del entorno operativo actual y futuro, y las implicaciones para las FAS, el concepto aborda las **recomendaciones en los diferentes factores MIRADO-I**[1] que

[1] Material, Infraestructura, Recursos humanos, Adiestramiento, Doctrina, Organización, Interoperabilidad

orientarán la nueva capacidad C-UAS LSS, e identifica los requisitos básicos que deberían tener los elementos que apoyen esta capacidad.

09. El concepto es lo suficientemente **flexible** para poder evolucionar al mismo ritmo que lo haga la amenaza, manteniendo la iniciativa para garantizar la protección y libertad de acción de las FAS.

10. El **espacio de la solución** se corresponde con el del ámbito del JEMAD, pudiendo suponer la modificación de actuales directivas, instrucciones u otros documentos promulgados. Asimismo, por considerarlo imprescindible y en línea con las directrices contenidas en la DDC 01/2018, se presentan propuestas que exceden el ámbito de las competencias del JEMAD.

11. El Concepto está alineado y **es compatible** con las iniciativas actuales en el marco de la OTAN y de la UE, así como con los desarrollos en curso que se realizan en el entorno del proyecto CONDOR de la DGAM y de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

4. METODOLOGÍA.

12. Los trabajos para el desarrollo del Concepto C-UAS LSS se han basado en la **metodología *CD&E*** (*Concept Development & Experimentation*), que contempla "*la sucesión de actividades enfocadas a la identificación, elaboración, depurado y validación de soluciones a problemas que, mediante la aplicación de* ***pensamiento creativo*** *y una* ***metodología analítica****, describen cómo una fuerza empleará nuevas capacidades o capacidades ya existentes (MIRADO-I) para operar en un ambiente dado, existente o previsto*".[2]

13. En la elaboración del Concepto C-UAS LSS han participado activamente numerosos **expertos** provenientes de organismos del Ministerio de Defensa [3](MINISDEF), Secretaria de Estado de Seguridad, la Industria[4] y la Academia[5], así como personal de apoyo de ISDEFE, *Semantia Lab*[6] y el Instituto Tecnológico la Marañosa (equipo del proyecto de acuerdo con el "Anexo E"), trabajando de forma colaborativa bajo la coordinación y liderazgo del CCDC.

14. El proyecto ha incluido las **fases** de Definición, Investigación, Descubrimiento & Desarrollo, Experimentación y Consolidación (figura 1) que se encuentran explicadas en el "Anexo D".

[2] JEMAD, PDC-01(A) "Doctrina de empleo de las FAS". Madrid, 27 de febrero de 2018. Párrafo 187.
[3] Ejército de Tierra, Armada, Ejército del Aire, Estado Mayor Conjunto, Mando de Operaciones, Centro de Inteligencia de las FAS, DGAM, Dirección General de Personal, Dirección General de Enseñanza y Reclutamiento, CENCIED.
[4] CENTUM, INDRA, ART Radar, Thales España, Escribano *Mechanical & Engineering*, IECISA.
[5] Facultad de Derecho de las Universidades de Murcia y Navarra, Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid.
[6] Empresa colaboradora con ISDEFE experta en el diseño de cuestionarios, la recogida y análisis de datos.

Figura 1: Fases proyecto. Metodología CD&E

5. ANÁLISIS DEL PROBLEMA.

5.1 El Entorno Operativo.

15. El desarrollo exponencial de las tecnologías de ocio y entretenimiento aplicadas al sector de los UAS LSS; la gran oferta en el mercado, facilidad de adquisición, su bajo coste y la sencillez del manejo; las capacidades de las plataformas y sus sensores; la falta de medidas de control de los UAS LSS y los operadores para garantizar el cumplimiento de la normativa; la falta de concienciación de los operadores; el empleo innovador por actores estatales y no estatales, han producido una gran proliferación en el uso de UAS LSS, provocando un **cambio en el entorno operativo** que se hace más patente aún en el entorno urbano.

Figura 2: Proliferación del empleo de UAS LSS civiles

16. En esta situación, numerosos factores influyen en la aparición del problema, algunos con mayor incidencia en la **amenaza** que representa el empleo hostil o malicioso de los UAS LSS de forma intencionada, y otros más relacionados con el **riesgo** que supone su uso imprudente.

17. Este nuevo entorno operativo, caracterizado por la incertidumbre, unos límites difusos, la presencia de la población civil y el componente tecnológico[7], nos obliga a ir más allá de la necesidad de adaptación a los cambios. No es suficiente con adaptarse, sino que habrá que hacerlo con rapidez y facilidad, es decir, con **agilidad**.

5.2 Implicaciones del Entorno Operativo para las FAS.

18. En los últimos años, las FAS y las FCSE de numerosos países han tomado **conciencia** de la amenaza emergente que supone el **empleo de UAS LSS de forma hostil,** contra fuerzas e instalaciones militares y civiles por parte de adversarios[8].

19. La responsabilidad de la vigilancia, control y defensa del espacio aéreo de soberanía española, así como el control de la circulación aérea general en tiempos de conflicto armado, corresponde al MINISDEF[9], en particular al **Mando de Defensa y Operaciones Aéreas** (MDOA)[10], lo que, unido a la necesidad de proteger su personal, medios e instalaciones, obliga a las FAS a dotarse de capacidad de respuesta a esta amenaza.

20. Nos hallamos ante una **amenaza creciente** para la seguridad, que supone un reto tanto tecnológico como institucional para disponer de sistemas, procedimientos y organización capaces de hacerle frente con eficacia y seguridad en los diferentes escenarios y entornos, y de evolucionar al mismo ritmo que lo hacen los propios UAS LSS.

21. El estudio de esta carencia de capacidad se enmarca en el **entorno operativo actual y futuro**. A la vista de la rápida evolución tecnológica en esta área, es previsible que la amenaza se haga más patente y compleja en los escenarios operativos a medio y largo plazo, lo que afectará negativamente a la protección y libertad de acción de la fuerza.

5.3 Categorización de la amenaza.

22. Existen **múltiples clasificaciones**[11] de los UAS en función del peso, altitud de vuelo, radio de acción, etc., y en general las diferentes clases y categorías de UAS se establecen en relación con el peso máximo al despegue.

23. Sin embargo, debido a la exponencial proliferación cuantitativa y cualitativa de los UAS LSS y las posibilidades de modificación, algunas de estas clasificaciones se han quedado un tanto **anticuadas** y, en este sentido, resulta complicado establecer una categorización de la amenaza que sea perdurable y que no esté sujeta a constantes actualizaciones.

---

[7] JEMAD, CEFAS "Concepto de empleo de las FAS 2017", cambio 2, Madrid 30 de mayo de 2018. Pág. 13.

[8] "*Adversario es el conjunto de actores de un conflicto a los que se les reconoce como potencial o abiertamente hostiles para los intereses propios o aliados y contra los cuales se puede prever el uso de la fuerza*". PDC-01(A). Óp. Cit. Párrafo 337.

[9] Ley 21/2003, de 7 de julio, de Seguridad Aérea.

[10] Orden Ministerial 86/2012, de 4 de diciembre, por la que se crean el Mando de Vigilancia y Seguridad Marítima y el Mando de Defensa y Operaciones Aéreas.

[11] Por ejemplo, dentro de la Clase I de hasta 150 Kg, las Categorías establecidas en el Reglamento de la Circulación Operativa (RCAO) son las siguientes: MICRO < 66 J, MINI <15 Kg, SMALL 15- 150 Kg), que son diferentes a las establecidas en la OTAN (MICRO < 2 Kg, MINI 2-20 Kg, SMALL > 20 Kg), o las establecidas para el US Army en su estrategia C-UAS (MICRO/MINI < 20 lb (9 Kg), SMALL TACTICAL 21-55 lb (9.5-25 Kg).

24. Por lo tanto, **a los efectos de este concepto**, la categorización de la amenaza UAS LSS se centrará en aquellos sistemas que, debido a sus características de reducida superficie equivalente radar, baja firma infrarroja y/o acústica, o vuelo a baja altura y velocidad, hacen que se sitúen **fuera de la envolvente** de detección, seguimiento, identificación y neutralización de los sistemas actuales de Defensa Aérea[12] (DA).

5.4 Enunciado del Problema.

25. Debido a las características de la amenaza categorizada anteriormente, los medios actuales de DA y de Protección de la Fuerza (PF) **no resultan eficaces** para garantizar la protección y libertad de acción de las FAS, en los dos escenarios fundamentales en las que éstas se desenvuelven:

- **Unidades e instalaciones militares en operaciones fuera del territorio nacional**. Existe una percepción creciente de amenaza debido a la evolución del empleo hostil de UAS LSS, desde su utilización como sensores de vigilancia de la actividad propia, hasta el uso como vector de armamento improvisado.
- **Unidades e instalaciones militares dentro de territorio nacional.** Factores tales como el entorno urbano, la presencia de población civil, la proliferación del uso recreativo de estos sistemas, la posible vulnerabilidad de las infraestructuras críticas y la alarma social que podría provocar esta amenaza en territorio nacional, implican una mayor complejidad y la aparición de nuevos aspectos a considerar.

26. **Enunciado del PMO:** "*Las FAS no disponen de una capacidad integral que permita prevenir, detectar, identificar, decidir y, en su caso, neutralizar los UAS LSS que, operando por fuera de las capacidades de la Defensa Aérea integral, son empleados de forma hostil o imprudente contra las unidades desplegadas en operaciones e instalaciones militares, dentro y fuera de territorio nacional*".

6. IDEA CENTRAL: INTEROPERABILIDAD[13].

27. De los trabajos realizados durante las fases de Investigación, Descubrimiento y Desarrollo, se llegó a la conclusión de que el factor fundamental que debía guiar el desarrollo de la capacidad C-UAS LSS, debía ser su interoperabilidad con las capacidades ya existentes.

28. El desarrollo exponencial de la tecnológica previsto a corto plazo, hace pensar que los sistemas C-UAS LSS existentes quedarán obsoletos en un breve periodo de tiempo. Por lo

[12] "*El Ejército del Aire es el responsable, en su misión con carácter permanente, de la vigilancia del espacio aéreo y del control del espacio aéreo de soberanía, con la finalidad de evitar un uso indebido o ilícito del espacio aéreo de soberanía nacional. Para ello, mantiene funcionando continuamente el Sistema (permanente) de Mando y Control Aéreo que proporciona la necesaria detección, identificación, información, control de interceptación y acometimiento sobre vectores aéreos (aeronaves, RPA y misiles), dentro de su alcance de detección, cuando la situación así lo requiere".* Jefe de Estado Mayor del Aire. Instrucción General 00-1 "Doctrina Aeroespacial Básica". 1ª Rev. Madrid. 29/11/2018. Vigilancia y Control del espacio aéreo. Pág. 26.

[13] "*La interoperabilidad (I) es la capacidad de operar* ***interconectado e integrado*** *con otras capacidades, organizaciones y organismos; es una cualidad que deben poseer todos los componentes de cada capacidad y, por lo tanto, debe ser considerada como parte de los mismos*". JEMAD, PDC-01(A). Óp. Cit. Párrafo 179.

tanto, es necesario desarrollar una capacidad C-UAS LSS que sea lo suficientemente **flexible** para poder adaptarse con agilidad a la evolución tecnológica de la amenaza.

29. Por tanto, resulta esencial adaptar los sistemas C-UAS LSS ante la gran velocidad de los cambios tecnológicos aplicados y para conseguirlo, será necesario un **ciclo continuo** de investigación-desarrollo-innovación-producción.

30. La solución al problema planteado debe afrontarse de una forma **coordinada** por parte de los responsables de proporcionar la defensa contra esta nueva amenaza en cada uno de los escenarios. El grado de coordinación, tanto en el ámbito de las FAS, como con otros organismos del Ministerio de Defensa y de la Administración del Estado, así como con las Organizaciones Internacionales en las España participa, dependerá del **grado de interoperabilidad** requerido para cada escenario y actores implicados.

31. Los sistemas C-UAS LSS deberán tener la capacidad de ser **interoperables** con los sistemas de DA y de PF existentes, empleando distintos grados de interconexión e integración dependiendo del escenario, entorno y tipo de protección. **Sumar esfuerzos para multiplicar resultados**.

6.1 Hipótesis.

32. **HIPÓTESIS ("Interoperabilidad"): SI** los sistemas C-UAS LSS operan interconectados e integrados con los sistemas de las capacidades de Defensa Aérea y de Protección de Unidades, Bases e Instalaciones.

    ENTONCES se mejorará la **eficacia** de la protección y libertad de acción de las FAS, ante la amenaza de UAS LSS empleados de forma hostil o imprudente contra unidades e instalaciones militares.

7. RECOMENDACIONES DE LOS FACTORES MIRADO - I.

33. A continuación, se presentan las recomendaciones de los diferentes factores MIRADO-I, derivadas del proceso metodológico efectuado durante el desarrollo del concepto, que deberían orientar la elaboración del **Plan de Implementación** que desarrolle la capacidad[14] integral de Defensa C-UAS LSS.

7.1. Materiales.

34. **No existe una única solución tecnológica C-UAS LSS** que sea efectiva contra toda amenaza en todo momento y lugar, sino que se deberá considerar qué tipo de sistema es más adecuado para cada escenario de empleo de las FAS, entorno y situación general del objetivo a proteger.

[14] "*Se entiende por Capacidad Militar al conjunto de sistemas que, operados bajo unos principios y procedimientos doctrinales establecidos, permiten obtener determinados efectos mediante su empleo en operaciones para cumplir con las misiones asignadas*". JEMAD, PDC-01(A) Loc. Cit. Párrafo 169.

35. En este sentido, para la protección de las bases unidades e instalaciones militares dentro de territorio nacional, destacan las **bases aéreas** por su complejidad e impacto que podría llegar a tener la acción de UAS LSS sobre la actividad aérea que en ellas se desarrolla.

36. Asimismo, la protección de los **buques de la Armada**, tanto atracados y durante las entradas y salidas de puerto, como durante las navegaciones por aguas restringidas cercanas a costa, requerirá de sistemas C-UAS LSS adecuados a dichas situaciones.

37. Un sistema C-UAS LSS se puede definir como un "**sistema de sistemas**" formado por diferentes sensores, sistema de mando y control (C2) y sistemas de armas, para las diferentes fases del **ciclo C-UAS LSS:** prevención, detección, identificación, decisión y neutralización[15].

Figura 3: Ciclo sistemas C-UAS LSS

38. Para cada una de estas fases, existen diferentes tecnologías y sensores disponibles en el mercado o en desarrollo, que se encuentran explicados en detalle tanto en el **estudio prospectivo sobre tecnología**[16], donde se exponen aquellas tecnologías que pueden tener un papel importante en la evolución de las diferentes fases del ciclo de los sistemas C-UAS LSS, como en el **informe del Análisis Base**[17], donde se exponen las ventajas e inconvenientes que presenta cada tipo de sensor.

39. Los sistemas C-UAS LSS deberán ser **modulares, escalables, actualizables** rápidamente para adaptarse a la evolución de la amenaza; que permitan la **integración de diferentes tipos de sensores** para la detección, identificación, decisión, y de **sistemas de armas** para la neutralización; que se basen en la **cooperación de tecnologías** complementarias (radar, optrónica, acústica, energía dirigida, submuniciones, etc.); que tengan fácil **movilidad** y requerimientos mínimos para su puesta en funcionamiento tras un cambio de ubicación.

[15] A efectos del concepto, se entiende por neutralización la fase final de la defensa C-UAS LSS con el objetivo de perturbar, controlar o destruir la amenaza, mediante el empleo de sistemas de armas cinéticas y no-cinéticas.
[16] CCDC. "Documento Grupo de Trabajo de Tecnología". Concepto Nacional C-UAS. Madrid, 6 de junio de 2018. Apartado 4. Pág. 7-10.
[17] CCDC. "Análisis Base". Concepto Nacional C-UAS. Madrid, 16 de julio de 2018. Apartado 4.d. Pág. 25-30.

40. Los sistemas C-UAS LSS más complejos deberán disponer de un **alto grado de automatización**, que permita un proceso de la decisión ágil. Debido al escaso tiempo de respuesta del que disponen los sistemas C-UAS LSS, las fases de detección, identificación y la recomendación de decisión deberían realizarse de forma automática. La fase de neutralización se debería poder configurar en **modos de operación** manual, semiautomático y automático, dependiendo de la amenaza, escenario, entorno, situación, estado de alerta y reglas de enfrentamiento (ROE) en vigor.

41. Si bien los sistemas C-UAS LSS podrían llegar a tener la capacidad de interconectarse e integrarse mediante un sistema de C2 con el resto de los sistemas de DA y de PF, se considera que en el corto y medio plazo la integración debería ser como mínimo a **nivel local** de cada sistema C-UAS LSS, para asegurar un **ciclo de decisión** del operador adecuado en cuanto a la neutralización o no del UAS LSS detectado. Hasta que la tecnología no permita una integración completa de los sistemas C-UAS LSS en el Sistema de Defensa Aérea[18] (SDA), ésta se llevará a cabo mediante procedimientos y comunicaciones directas.

42. Se deberá buscar la **sencillez** en la operación y el mantenimiento, con el fin de que su empleo solo requiera un determinado nivel de especialización y no de especificidad, reducir las necesidades de Instrucción y Adiestramiento (I+A) y la huella logística para el despliegue.

43. Los sistemas C-UAS LSS deberán tener un **alto grado de disponibilidad operativa**, que les permita su funcionamiento en ciclos de 24/7, lo que requerirá de sistemas con una alta fiabilidad y mantenimientos programados que se puedan ejecutar con rapidez.

44. La capacidad C-UAS LSS debe ir más allá de los sensores y sistemas de armas necesarios para la detección, identificación y neutralización de los UAS LSS. Se considera necesario actuar contra el adversario que ha decidido emplearlos de forma hostil contra nuestras FAS. Para ello, la **explotación técnica** de la información obtenida de los componentes y capacidades de los UAS LSS neutralizados, apoyaría la fase de prevención del ciclo C-UAS LSS.

45. Se deberá mantener una **vigilancia de los desarrollos tecnológicos** de los UAS LSS, como mínimo en el horizonte del medio plazo, para asegurar que la nueva capacidad C-UAS LSS se mantenga actualizada con respecto a esta amenaza que se prevé que evolucione con gran rapidez.

7.2. Infraestructura.

46. Las necesidades de infraestructura vendrán **condicionadas** por el tipo de sistema C-UAS LSS (portátil/fijo/móvil), los diferentes sistemas que lo compongan (sensores de detección e identificación, sistema C2, sistema de neutralización) y el nivel de integración que se determine (aislado, local, C2, total). Se considera que el mantenimiento de los sistemas C-UAS LSS se podría realizar en las infraestructuras actuales. No obstante, se debería procurar

[18] "*Así la defensa aérea se basa en la integración de sensores, plataformas y armas y en los automatismos, apoyados con la transferencia de datos, que permiten la formación de un sistema integrado de defensa aérea*". Instrucción General 00-1. Óp. Cit. Anexo B. Pág. 9.

que las necesidades de instalación sean las mínimas posibles y limitadas al emplazamiento físico del sistema.

47. Además de las necesidades de infraestructura de los propios sistemas C-UAS LSS, habrán de tenerse en cuenta las necesidades de infraestructuras de **ocultación y protección física** para el personal y los elementos críticos de las instalaciones a proteger.

48. Asimismo, habrá que considerar las **necesidades de I+A** relativas a infraestructura, derivadas de la implementación de esta nueva capacidad, para actualizar las instalaciones de adiestramiento existentes (campos de maniobras, simuladores, etc.).

7.3. Recursos Humanos.

49. Disponer de personal específico dedicado a las funciones y cometidos C-UAS LSS aumentaría la eficacia en el empleo de estos sistemas. Sin embargo, teniendo en cuenta el resto de las necesidades de las unidades y atendiendo a requerimientos de eficiencia de personal, se considera que la operación y el mantenimiento de los sistemas C-UAS LSS debería ser asumido por **personal especializado** que, dentro de sus unidades y cometidos ya asignados, también asuma estas nuevas funciones.

50. Los requerimientos para determinar las soluciones tecnológicas deben definirse de forma que se busque la **sencillez de operación y mantenimiento** de los sistemas C-UAS LSS, con el fin de que su empleo solo requiera determinado nivel de especialización y no de especificidad. De esta forma, los sistemas C-UAS LSS serían una capacidad más de las unidades y no se requeriría disponer de personal dedicado en exclusiva a los mismos.

51. El personal necesario para operar y mantener los sistemas C-UAS LSS dependerá del tipo de sistema a emplear (portátil/fijo/móvil), del nivel de integración con los sistemas de DA y de PF, así como de la situación general de defensa requerida (protección permanente de un objetivo fijo, temporal de un objetivo fijo o temporal de uno móvil)[19]. No obstante, se debería tender a que el mismo personal que opera el sistema también sea capaz de realizar al menos el mantenimiento mínimo, de primer escalón.

52. En general, los **sistemas portátiles y móviles** normalmente se emplearán para la protección temporal de objetivos fijos o móviles, por lo que podrían ser manejados por personal con responsabilidades de PF, ya sea de forma dedicada o puntualmente como un cometido adicional cuando el nivel de amenaza lo requiera.

53. Por el contrario, los **sistemas fijos** normalmente se emplearán para la protección de objetivos fijos de forma permanente, por lo que el personal responsable de la seguridad debería tener la formación especializada para operar los diferentes sistemas que lo formen, en sus diferentes fases: detección, identificación, decisión y, llegado el caso, neutralización del UAS LSS amenaza.

[19] Escenarios, entornos y tipos de protección conforme a lo definido en el “Anexo C”.

7.4. Adiestramiento.

54. El requisito previo al adiestramiento en el manejo de los sistemas C-UAS LSS, es **concienciar** al personal de las FAS sobre las implicaciones que tiene esta amenaza en el entorno operativo. Debería iniciarse cuanto antes y mantenerse de forma permanente en las enseñanzas de formación y específica. Para ello, es fundamental desarrollar un **plan de I+A** en escenarios que incluyan la amenaza de UAS LSS hostiles combinados con UAS propios, para practicar las tácticas, técnicas y procedimientos (TTP) y las medidas de protección y respuesta establecidas, mediante ejercicios individuales y colectivos.

55. Las necesidades de I+A tendrán que desarrollarse en los respectivos **procesos de formación** orientados tanto al personal operador desde un punto de vista táctico, como al personal de carácter técnico para el mantenimiento de los sistemas C-UAS LSS, así como al personal responsable de la toma de decisiones en los puestos de C2. Además, se debería incluir el empleo de esta nueva capacidad en los cursos relacionados con las operaciones.

56. Para el diseño de los planes de formación de operadores y personal técnico, se podría tomar como **referencia inicial** el plan de formación de los sistemas C-UAS LSS de la solución interina. Asimismo, se considera conveniente que el personal operador de sistemas C-UAS LSS, también recibiera formación en materia de TTP de los UAS LSS en servicio en nuestras FAS, con objeto de comprender mejor la amenaza.

57. Se considera conveniente orientar la I+A a **diferentes niveles** orgánicos de los Ejércitos, para abarcar desde el desarrollo de las habilidades del personal para identificar visualmente los UAS LSS enemigos, hasta la realización de ejercicios a nivel conjunto:

- **Adiestramiento individual**, de familiarización del personal con las capacidades de los UAS LSS y la amenaza que suponen para la unidad, así como la manera de identificar signos de actividad enemiga asociada a la misma y la respuesta inmediata.
- **Adiestramiento de unidad**, de preparación colectiva de la unidad para detectar, identificar, responder e informar ante la amenaza de UAS LSS.
- **Adiestramiento conjunto**, de ejercicios conjuntos con otras unidades para practicar procedimientos de información, coordinación, en particular con el SDA.

58. El **adiestramiento individual y de conjunto** en la defensa C-UAS LSS sería similar al que se realiza contra otras amenazas, principalmente las relacionadas con las operaciones de Defensa Antiaérea. Los ejercicios contra UAS LSS deberían estar estandarizados y realizarse tanto a nivel específico como conjunto.

59. Para la formación de los operadores de sistemas C-UAS LSS, se considera que el empleo de **simuladores** para practicar las TTP ante esta nueva amenaza de forma integrada en los escenarios de actuación, ayudaría a alcanzar los objetivos de adiestramiento.

60. En relación con el escenario general de actuación de **Seguridad nacional ampliada**, considerado como el más exigente, en el que las FAS proporcionan bien una respuesta específica o contribuyen a una respuesta general como parte de la Acción del Estado, se debería establecer la coordinación necesaria con el resto de los organismos del Ministerio de Defensa y otros Ministerios relacionados con la Acción del Estado, en aras de alcanzar y mantener la necesaria interoperabilidad. Esta coordinación se podría materializar

mediante acuerdos y sus respectivas comisiones de seguimiento, para establecer los planes de preparación ante la amenaza, la realización de **ejercicios conjuntos** con las FCSE o incluso la generación de estructuras interministeriales para coordinar esfuerzos.

61. En definitiva, será necesario mantener una **formación constante** tanto en la operación como en el mantenimiento de los sistemas C-UAS LSS, capaz de evolucionar al mismo ritmo que lo haga esta amenaza basada en sistemas tecnológicos novedosos, con especial énfasis en acciones formativas específicas previas a las operaciones.

7.5. Doctrina.

62. La nueva capacidad C-UAS LSS implicará tener que **revisar y adaptar la doctrina existente** conjunta, específica y combinada, sobre la utilización de las diferentes capacidades afectadas por la misma, así como analizar la posibilidad de creación de una doctrina particular. La evolución será muy rápida, por lo que se debería desarrollar en paralelo a los nuevos sistemas, para que la solución al problema no pierda eficacia o se quede obsoleta en un corto periodo de tiempo.

63. Para garantizar la eficacia de los sistemas C-UAS LSS será necesario tener en cuenta los **puntos de vista técnico y táctico,** adecuando y aplicando la doctrina y procedimientos de DA, gestión del espacio aéreo y PF.

64. Si bien esta nueva capacidad afecta a las **capacidades** representadas en la figura 4, se considera que el problema que supone enfrentar los UAS LSS empleados de forma hostil contra fuerzas e instalaciones militares, se puede abordar desde una doble orientación dependiendo del escenario, entorno y situación: **DA** o **PF.**

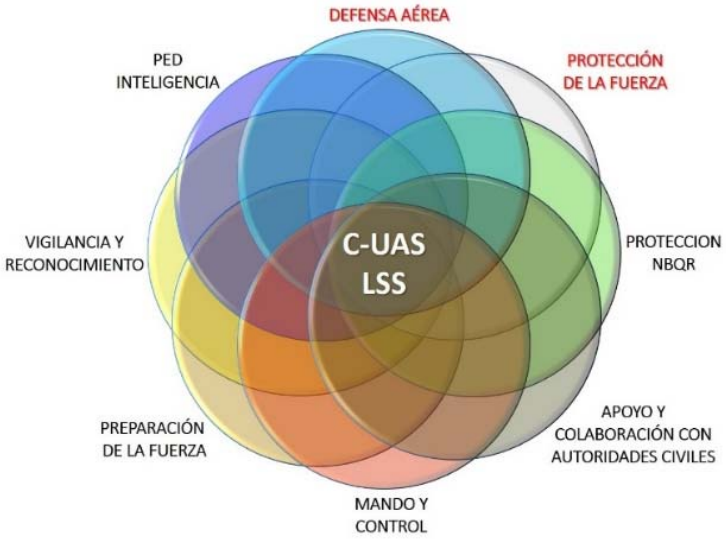

Figura 4: Áreas de capacidad afectadas por la defensa C-UAS LSS

65. Por un lado, la doctrina de la **DA**[20], con sus principios[21]y fundamentos, permite aplicar gran parte de la **experiencia**[22] adquirida y que ha sido instruida y adiestrada a través de los procedimientos existentes.

66. Por otro lado, la doctrina de **PF**[23] aplica procedimientos de **gestión del riesgo** y adopta medidas de protección pasiva y activa para contrarrestar las distintas amenazas. Incluye medidas preventivas de control del área de responsabilidad, disuadiendo al adversario o negando a éste su capacidad de ataque. Asimismo, aplica el principio de atacar la red del adversario, para lo que es fundamental disponer de la capacidad de explotación técnica del incidente UAS LSS, de la que se obtendrá la información para elaborar la inteligencia que permita atacar esas redes.

67. Las características de la defensa C-UAS LSS, que implica distancias de detección reducidas y un escaso tiempo de reacción, hacen que esta amenaza haya de ser enfrentada por la PF cuando los sistemas de Defensa Antiaérea (DAA) no sean capaces de afrontarla o no se disponga de ellos, siguiendo las normas de coordinación emanadas del Jefe de la DA y siempre que sea posible integradas en la capacidad de DA.

68. Por otra parte, desde el **punto de vista jurídico** podría ser más conveniente dar cobertura legal, fijar responsabilidades y justificar las actuaciones de los sistemas C-UAS LSS, como

---

[20] En el nivel operacional, la defensa contra amenazas aéreas está incluida en la función conjunta "fuegos". JEMAD. PDC-01 (A). Óp. Cit. Pág. 129. Párrafo 548.
La definición de Defensa Aérea en la OTAN es: "*Air Defence/défense aérienne AD: all measures designed to nullify or reduce the effectiveness of hostile air action. AAP-06 (2018) NATO Glossary of term and definitions.* Pág. *5*.
De acuerdo a la Doctrina Aeroespacial del Ejército del Aire, "*La defensa aérea puede ser activa o pasiva. La defensa aérea activa incluye las acciones llevadas a cabo contra las fuerzas del adversario, en forma de amenaza aérea o de misiles, para anularla o para reducir la efectividad de cualquier ataque. Se caracteriza, usualmente, por una defensa en profundidad en capas que permite múltiples oportunidades de enfrentamiento, utilizando sensores, aeronaves y sistemas de superficie. Así, la defensa aérea se basa en la integración de sensores, plataformas y armas y en los automatismos, apoyados con la transferencia de datos, que permiten la formación de un sistema integrado de defensa aérea. La defensa aérea pasiva incluye las medidas no activas, que mejoran la supervivencia, para la defensa física y la protección del personal, instalaciones y equipos esenciales con el fin de minimizar la efectividad de los ataques aéreos y/o de misiles del adversario. Incluye la alerta temprana; el camuflaje, ocultación, dispersión y engaño; el endurecimiento de estructuras; la movilidad; la dispersión; la redundancia; la utilización de equipamiento e instalaciones de protección NBQR; la adopción de tecnologías de baja detectabilidad (stealth) y políticas de control de emisiones*". Instrucción General 00-1. Óp. Cit. Anexo B. Pág. 9.

[21] Control de la situación aérea, negar la inteligencia, alerta temprana, defensa en profundidad, integración de la defensa aérea, planeamiento centralizado y ejecución descentralizada. MADOC del ET. PD3-311. "Defensa Antiaérea". Pág. 2-1.

[22] "*El empleo de RPAS civiles está generando una nueva amenaza, que se debe combatir adaptando los procedimientos de actuación en vigor y complementando las capacidades de los materiales en servicio, pero aprovechando la experiencia y mentalidad de las actuales unidades Ground Based Air Defence*". MADOC ET. DIDOM-IV-017. "Tendencias Vol. I. Aspectos Generales". Granada, diciembre 2017. Pág. 84

[23] "*La Protección de la Fuerza engloba aquellas actividades que tienen como objeto minimizar la vulnerabilidad del personal, equipo, material, instalaciones, información, operaciones y actividades de la Fuerza y de los elementos no militares que apoyan, acompañan o están bajo responsabilidad de la Fuerza, frente a las acciones adversarias, propias, y frente a los riesgos sanitarios, naturales, tecnológicos y accidentes. Su finalidad es preservar la libertad de acción del Comandante y garantizar la operatividad de la Fuerza*". JEMAD. PDC-3.14(A) "Protección de la Fuerza" (borrador). Madrid. NOV 2018. Párrafo 014.

parte de la capacidad de PF, al tener similitud con el área de seguridad ciudadana del Ministerio del Interior.

7.6. Organización.

69. Como ya se ha indicado, a la hora de orientar la integración de la futura capacidad de defensa C-UAS LSS, existen **dos capacidades** (PF y DA) susceptibles de abordar la amenaza de forma complementaria. Las conclusiones extraídas de la fase de experimentación[24] del proyecto, indican que en términos generales **no existen grandes diferencias** entre el planeamiento de una operación desde un enfoque de DA o de PF, si bien se aprecia que existen diferencias dependiendo del escenario donde se presente el problema.

70. En el caso de un **escenario terrestre**, las variables analizadas[25] durante el experimento realizado, excepto la de gestión integrada del espacio aéreo y la de interferencia en la misión principal, aconsejan el planeamiento basado en PF. No obstante, la necesaria unidad de doctrina a nivel conjunto y la importancia de las variables mencionadas anteriormente, imponen que el planeamiento en el componente terrestre se base en DA.

71. Para un **escenario marítimo** se considera que, allí donde puede hacerse uso de los sensores de DA de los buques, el enfoque de DA obtendría unos mejores resultados que el de PF. Sin embargo, si la navegación transcurre cerca de costa o el buque no dispone de tales medios, el enfoque de PF podría ser más adecuado.

72. Finalmente, para un **escenario aéreo**, se observa una mayor paridad en ambos enfoques, si bien, al igual que en el caso del escenario marítimo, la orientación desde DA requiere adaptar los procedimientos actuales a la amenaza UAS LSS, pues se considera que la estructura de DA permite acoger distintos niveles de decisión y ejecución dependiendo de las circunstancias y del escenario.

73. En definitiva, se considera que la integración más eficaz de la capacidad C-UAS LSS sería desde un **enfoque mixto y complementario** que, cuando la solución se oriente desde la perspectiva de PF, dependiendo del escenario y los medios asignados, haga uso de los sistemas disponibles de DA de manera coordinada con el SDA.

74. En zona de operaciones, para la defensa de unidades e instalaciones militares fijas (bases terrestres, navales y aéreas, etc.), se podría tomar como referencia la idea de **Unidades de Artillería Antiaérea**, como una organización operativa generada para un espacio, lugar y tiempo determinados contra una amenaza aérea determinada (en este caso UAS LSS). En cambio, para la defensa de instalaciones militares fijas en territorio nacional, la organización podría basarse en las **Unidades de Seguridad**, que incluirían en sus procedimientos los correspondientes a la Defensa Antiaérea integrada.

75. Tomando como modelo el ámbito C-IED, se considera conveniente contar con una **estructura de coordinación** a nivel estratégico que centralice las diferentes áreas de interés

[24] El diseño, ejecución, resultados, análisis y conclusiones de la fase de experimentación se encuentran en el documento "Informe Experimentación Concepto C-UAS LSS". CCDC, Madrid, 10 diciembre 2018.

[25] Eficacia de la defensa, cobertura de la protección, tiempo de reacción, probabilidad de daños colaterales, grado de interferencia en la misión principal, prevención, sostenimiento, flexibilidad, gestión integrada del espacio aéreo.

relacionadas con la amenaza de UAS LSS, como la concienciación del personal, la formación especializada en la operación y mantenimiento de los sistemas, la explotación técnica de los UAS LSS neutralizados, la experimentación y simulación, los estudios sobre tecnología y evolución de la amenaza, la coordinación con las FCSE y con las FAS de otros países, etc.

76. Asimismo, a la vista del aumento de incidentes en países de nuestro entorno, se estima necesario disponer de una **organización a nivel nacional** responsable de la coordinación de las acciones contra la amenaza UAS LSS que deban realizar los distintos organismos competentes de la Administración del Estado. En el ámbito de las FAS, se considera que este podría ser el AOC (*Air Operations Center*) del MDOA a través de una célula C-UAS LSS, el que coordinara las acciones contra UAS LSS de aquellas unidades dotadas con dichos medios, descansando en ellas la responsabilidad de neutralización de la amenaza, de acuerdo al principio de ejecución descentralizada.

7.7. Interoperabilidad.

77. Los sistemas C-UAS LSS deberían ser capaces de operar **interconectados** con los sistemas de C2 del nivel táctico de DA y de PF, de manera que puedan compartir la información necesaria y realizar el planeamiento y conducción de las operaciones C-UAS LSS.

78. Se considera que debería establecerse un **nivel mínimo de integración** de los sistemas C-UAS LSS a nivel local, debido al escaso tiempo de reacción para dar una respuesta eficaz. Sin embargo, se deberá tender hacia una integración a nivel de C2 con los sistemas de DA y de PF, que pueda evolucionar hacia el máximo nivel de integración posible que nos permita la tecnología, para lograr una visión global de la amenaza UAS LSS.

79. Por otro lado, es necesario buscar una **integración a nivel intelectual** además de la requerida a nivel técnico, tanto dentro de las FAS como también con los otros organismos de la Administración del Estado relacionados con la defensa C-UAS LSS, ya que en ambientes degradados (guerra electrónica, ciberataques, etc.) será más importante saber qué hacer, cómo y cuándo hacerlo.

80. Es esencial el **planeamiento integrado y colaborativo** de las capacidades de los sistemas C-UAS LSS con el resto de las capacidades, así como la inteligencia compartida entre todos los escalones. Se considera vital, potenciar la **capacidad de obtención y explotación de inteligencia**, en particular la explotación técnica de los UAS LSS neutralizados y capturados, incluyendo el intercambio de dicha información con las FCSE.

81. Es necesario establecer **procedimientos de coordinación** para el **apoyo a autoridades gubernamentales**, que permitan proteger los objetivos que se determinen dentro del territorio nacional, y compartir la inteligencia para prevenir la materialización de la amenaza. Para ello, y entre otros, se deberían establecer **estructuras** donde se materialice dicha coordinación, tanto para la fusión de información que permita una mejor decisión respecto de un incidente UAS LSS, como para el estudio de procedimientos, normativa, etc.

82. Respecto de la **neutralización** de los UAS LSS en territorio nacional, existen dos aspectos que han de ser tenidos en cuenta. Por un lado, la neutralización de la aeronave, que con arreglo a la normativa pudiera corresponder al MDOA (en el entendido que normalmente la unidad amenazada será la responsable de llevar a cabo tal neutralización), y por otro la

neutralización del operador, que fuera de las instalaciones militares correspondería a las FCSE.

83. Al igual que la cooperación entre FAS y FCSE en materia de la defensa C-UAS LSS dependerá del grado de integración de sus respectivos sistemas, en el ámbito interno de las FAS habrá que considerar la necesidad de que los diferentes sistemas C-UAS LSS que se decidan adquirir en el marco del proyecto CONDOR, tengan la capacidad de **operar interconectados e integrados**.

8. FACTORES ADICIONALES A CONSIDERAR.

84. Además de los factores MIRADO-I, se estima necesario incluir una serie de **factores adicionales** a considerar, fruto del análisis llevado a cabo en la fase de investigación del proyecto y del trabajo realizado por los expertos durante la fase de descubrimiento y desarrollo, por su importante contribución para dar una solución eficaz al PMO planteado.

85. Estos factores afectan principalmente al escenario de **seguridad del territorio nacional**, debido al mayor peso que tienen aspectos como el entorno urbano, la presencia de población civil, la proliferación del uso recreativo de estos sistemas, las responsabilidades de las FCSE, o la alarma social que podría provocar esta amenaza en territorio nacional.

86. Se considera, además, que las recomendaciones incluidas en estos factores adicionales **reducirían el riesgo** que supone el uso imprudente de los UAS LSS, facilitando identificar aquellas situaciones potencialmente peligrosas de causar daños al personal e instalaciones militares dentro del territorio nacional, debido al empleo hostil de forma intencionada.

8.1. Gestión integrada del espacio aéreo.

87. "*El posible uso de aeronaves pilotadas remotamente para acciones de naturaleza agresiva o ilícita por parte de Estados u organizaciones no estatales constituye un ejemplo actual que justifica la* ***protección del espacio aéreo***"[26].

88. La gestión integrada del espacio aéreo aporta importantes **beneficios** en la defensa C-UAS LSS. Proporciona alerta temprana ante amenazas UAS LSS, aumentando el tiempo mínimo disponible de reacción para proteger al personal y material, reduciendo los posibles daños y mejorando el ciclo de decisión propio frente al del adversario. Asimismo, permite el empleo coordinado de UAS LSS amigos en la zona, evitando interferencias entre los diferentes sistemas C-UAS LSS y que se produzcan incidentes de fuego amigo.

89. Sería deseable disponer de la información proporcionada por los **sistemas civiles de gestión del tráfico aéreo a muy baja altura**[27], para su posible integración a través del SDA en la situación aérea local de los sistemas C-UAS LSS, con el objetivo de tener una situación

[26] Presidencia del Gobierno de España. "Estrategia de Seguridad Nacional 2017. Un proyecto compartido de todos y para todos". Madrid, 2017. Pág. 70.

[27] Vuelos por debajo de la altura de coordinación (120 m sobre el terreno, tanto urbano como rural). Su funcionamiento se basa en una gestión centralizada de planes de vuelo, apoyada por una serie de servicios fundamentales como el registro electrónico, identificación electrónica y *geofencing*, cuyo desarrollo está siendo llevado a cabo actualmente por la Agencia *Single European Sky Air traffic management Research Joint Undertaking* (SESAR JU) de la UE.

aérea general de muy baja cota lo más completa posible, comunicar la alerta, adoptar medidas de protección inmediata del personal e instalaciones y asignar el medio de neutralización disponible más apropiado en el mínimo tiempo.

8.2. Concienciación.

90. Es necesario **percibir la amenaza como real y creciente**. El mal uso de los UAS LSS, ya sea de forma imprudente, o malintencionada con fines maliciosos y hostiles, supone un riesgo y amenaza real para la seguridad de las personas e instalaciones.

91. Se considera que existe un gran **desconocimiento de la normativa** en vigor sobre el empleo civil de los UAS, e incluso cierta reticencia o incapacidad para cumplir las normas establecidas. Las necesidades de concienciación sobre el uso los UAS LSS deberían orientarse a tres audiencias diferentes:

- **Política/estratégica**. Proporcionar al nivel político una visión real de la amenaza que suponen los UAS LSS (tanto para las propias FAS, como para la población). Si no se percibe como tal, será difícil disponer de los recursos necesarios para contrarrestarla.
- **Personal de las FAS**. Resulta fundamental que los miembros de las FAS sean conscientes de la proliferación de UAS LSS enemigos y propios en las operaciones y conozcan los procedimientos para actuar contra los UAS LSS que supongan una amenaza.
- **Usuarios de UAS comerciales.** Si bien no se considera una responsabilidad que deba liderar el MINISDEF, sí podrían tomarse medidas para aumentar la concienciación, sobre todo en zonas o poblaciones en las que haya instalaciones militares en los alrededores, u otras declaradas como críticas.

92. Esta labor de concienciación no debe limitarse a la difusión de la normativa que regula la utilización civil de los UAS LSS[28], sino extenderse a la difusión de información sobre las infracciones penales o administrativas en las que se podría incurrir cuando su vulneración lleve aparejada la violación de otras leyes[29].

8.3. Regulación Normativa.

93. Las implicaciones identificadas desde el punto de vista normativo en el concepto C-UAS LSS, afectan principalmente al escenario de operación **dentro del territorio nacional**. Se considera que es un tema de estudio fundamental en la búsqueda de la solución del PMO, debido a su contribución a la hora de evitar incidentes por el uso civil de UAS **de forma imprudente**, que provocan situaciones de peligro susceptibles de causar daños personales y materiales. El empleo imprudente está considerado como la amenaza más probable a la seguridad, representando la mayor parte de los incidentes de seguridad en la actualidad.

94. Es fundamental el desarrollo, establecimiento y aplicación de **normativas y requisitos de empleo y seguridad** para todos los actores, usuarios, fabricantes y organismos reguladores,

[28] Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto.
[29] Como por ejemplo la Ley 21/2003, de 7 de julio, de Seguridad Aérea, o la Ley 8/1975, de 12 de marzo, de zonas e instalaciones de interés para la Defensa Nacional.

que garanticen el uso seguro de los UAS LSS y que reduzcan al mínimo la posibilidad de incidentes por un uso imprudente, así como su **constante revisión** para que estos sistemas sigan aportando los beneficios que se esperan para los próximos años.

95. Se considera necesario desarrollar la normativa actual sobre el uso civil de UAS, para establecer **mecanismos de control** adicionales que ayuden a prevenir el posible uso de los UAS LSS con fines ilícitos y maliciosos, como por ejemplo, la posibilidad de identificación electrónica de las aeronaves en vuelo y sus estaciones de control en tierra. El establecimiento de un sistema de registro de UAS LSS con la identificación del titular de la compra, supondría una mejora en el control del uso recreativo y comercial.

96. La implementación de **sistemas de identificación electrónica y de *geofencing***[30], redundaría en la mejora de la seguridad. La identificación electrónica haría posible la detección de operaciones no permitidas de UAS LSS e incluso la identificación del operador mediante la explotación técnica de esta información. Por su parte, el *geofencing* ayudaría a limitar el sobrevuelo de infraestructuras críticas, instalaciones afectas a la defensa nacional o a la seguridad del Estado y otras zonas restringidas[31].

97. Por último, el empleo de sistemas C-UAS LSS en **operaciones en el exterior** estará sujeto, como regla general, a las normas del país en cuestión, en función de dónde y bajo qué circunstancias se desarrolle la operación, por lo que durante el planeamiento se tendrán que considerar las limitaciones o restricciones que se deriven.

8.4. Coordinación entre FAS y FCSE.

98. La solución a la forma de enfrentar la amenaza de UAS LSS dentro de territorio nacional tendrá múltiples factores, que requerirán una **respuesta coordinada** entre las FAS y las FCSE. Igualmente, es necesario considerar las diferentes restricciones de jurisdicción privada, límites geográficos, áreas de responsabilidad, etc.

99. El grado de **coordinación** dependerá de la posibilidad de integración de los respectivos sistemas C-UAS LSS en un único sistema C2, o de la interoperabilidad entre los sistemas C2 de ambas organizaciones. Otros aspectos que considerar son el adiestramiento conjunto para conocer las capacidades y TTP de cada uno, así como el intercambio de inteligencia relativa a la amenaza.

100. Actualmente, existe un **Grupo de Trabajo Interministerial sobre drones**[32] para aumentar la coordinación en los desarrollos de sistemas C-UAS LSS. Se considera necesaria la participación en dicho grupo de personal del EMAD responsable de la implementación del concepto C-UAS LSS.

[30] Zonas de acceso limitado mediante posicionamiento por satélite e identificación por radiofrecuencia.
[31] Ministerio de Fomento. "Plan Estratégico para el desarrollo del sector civil de los drones en España 2018-2021". Pág. 23.
[32] Liderado por el Área de Seguridad Ciudadana y Operaciones (ASCOP) del Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad, en el que participan representantes de la Guardia Civil, Policía Nacional, Ministerio de Defensa (a través de DIGENPOL), Ministerio de Fomento, Casa Real, Centro Nacional de Protección de Infraestructuras Críticas y Presidencia del Gobierno.

8.5. Aspectos legales y Éticos.

101. El ritmo acelerado con el que se producen los avances tecnológicos debido al crecimiento exponencial de las capacidades de las herramientas informáticas aplicadas a tecnologías, como la inteligencia artificial y los sistemas autónomos, está ocasionando el aumento de las preocupaciones sobre los **aspectos legales, los valores morales y los principios éticos**[33].

102. En este concepto únicamente se analiza la legalidad de la respuesta ante la detección de un UAS LSS, cuyo origen es considerado procedente de otro Estado o de algún grupo no estatal, desde el ámbito del uso de la fuerza **conforme al Derecho Internacional (DI)**, en los escenarios generales de Seguridad Exterior y Seguridad del Territorio Nacional.

103. Es preciso valorar las **normas que regulan el uso de la fuerza** mediante el empleo de los sistemas C-UAS LSS, con el objeto de establecer las condiciones en las que una acción concreta de un UAS LSS hostil o sospechoso puede originar una respuesta, qué tipo de respuesta y qué cobertura jurídica tendría dicha respuesta.

104. La situación es compleja, porque los UAS LSS podrían llevar a cabo un **amplio abanico de acciones hostiles o maliciosas**. En cada caso, la respuesta deberá ser diferente porque también es diferente el marco jurídico en el que ha tenido lugar su empleo[34].

105. La respuesta recomendada ante la incursión de un UAS LSS enviado por un Estado que llevara a cabo **acciones que no impliquen el empleo de la fuerza**, es, como regla general, el empleo de medidas que tampoco lleven aparejado un uso de la fuerza[35].

106. En el caso de que no fuera posible determinar con antelación suficiente si el UAS LSS pretende causar daños a gran escala o si las acciones fueran, de manera clara y sin lugar a duda, preparatorias de un ataque posterior de mayor escala, o fuesen susceptibles de ocasionar indirectamente "daños físicos" a las personas o a los bienes, se podría emplear la fuerza[36]. La respuesta más ajustada a Derecho sería la **neutralización**[37] del UAS LSS, aunque si no fuera posible hacerlo se podría proceder a su destrucción.

107. La **responsabilidad** jurídica civil y penal, interna e internacional por el uso de sistemas C-UAS LSS puede recaer en el gobierno, en la cadena de mando y en la persona concreta que

[33] *ACT "NATO Strategic Foresight Analysis 2017 Report", Norfolk*. Pág. 46. EMAD. "Entorno operativo 2035" septiembre 2018. Párrafo 218, Pág. 74.
[34] CERVELL HORTAL, María José. Documento de Investigación 11/2018, IEEE "La defensa contra sistemas aéreos no tripulados (C-UAS): Una reflexión jurídica preliminar desde el punto de vista del uso de la fuerza". Estudio académico colaboración en trabajos desarrollo Concepto C-UAS LSS. Junio 2018. Pág. 5.
[35] CERVELL HORTAL, María José. Loc. Cit. Pág. 6.
[36] GUTIÉRREZ ESPADA, Cesáreo. Documento de investigación 19/2018, IEEE "El desarrollo de un concepto conjunto de Defensa contra Sistema aéreos no tripulados (C-UAS) a la luz del Derecho Internacional de la Responsabilidad. Una aproximación preliminar". Estudio académico colaboración en trabajos desarrollo Concepto C-UAS LSS, septiembre 2018. Págs. 6-7.
[37] En principio, el uso de la fuerza (destrucción total del aparato) llevado a cabo contra un UAS LSS que se haya limitado a acciones de vigilancia o reconocimiento no es conforme al Derecho Internacional. CERVELL HORTAL, María José. Loc. Cit. Pág. 10.

autoriza o decide su empleo. Esto implica que quien autorice o decida el uso en un caso dado, debe asegurarse de que está en conformidad con la normativa mencionada.

108. Se considera necesario establecer y difundir unas **ROE** claras para combatir los UAS LSS, determinando las circunstancias, condiciones, grado y forma en las que se puede, o no, aplicar la fuerza, con especial atención a los posibles daños colaterales que pudieran ocasionarse por la neutralización de los UAS LSS.

109. La unidad mejor adiestrada, operando bajo una estructura perfecta, no puede lograr el éxito sin la **guía adecuada**, como son unas ROE perfectamente definidas. La aplicación de las ROE se verá dificultada cuando no se pueda identificar la carga útil del UAS LSS (si va armado o no), o no esté claro quién está pilotando la aeronave (su origen estatal o no estatal). Para ello, se deberán establecer unas consecuencias de empeño y consecuencias de interceptación que contemplen los daños colaterales que pudieran ocasionarse.

9. LÍNEAS FUTURAS.

110. Las conclusiones obtenidas tras el análisis de los resultados de la fase de experimentación del proyecto, han aportado valor al concepto por haber servido para comparar los dos enfoques diferentes para integrar la futura capacidad C-UAS LSS (PF y DA) y para comprobar otros aspectos de interés (automatización, integración). Sin embargo, se considera que dichas conclusiones deben tomarse con cautela, debido al reducido tamaño de la muestra impuesto por las limitaciones de tiempo y personal disponibles.

111. En este sentido se considera que, teniendo en cuenta la constante evolución de la amenaza UAS LSS debido al desarrollo exponencial de la tecnología y al empleo innovador que se hace de la misma, futuros experimentos realizados a corto plazo pudieran arrojar resultados diferentes.

112. Por tanto, resulta fundamental mantener un **seguimiento continuo de la evolución de la amenaza**[38], dado que sus características pueden incrementar los efectos de manera significativa a corto plazo. Factores tales como el aumento de las cargas útiles, autonomía, niveles de automatización, capacidad de enjambres, etc., pueden afectar significativamente a la forma de enfrentarse a los UAS LSS.

113. Por esta razón, está previsto realizar **campañas de experimentación** adicionales, que permitan avanzar en las consideraciones de material, contrastar las conclusiones alcanzadas en el experimento de alcance limitado llevado a cabo, así como evaluar la evolución de la amenaza y de las posibles soluciones para afrontarla.

114. Asimismo, se identifica la conveniencia de realizar una serie de **experimentos de validación** del concepto, en diferentes escenarios, entornos y situaciones, empleando UAS LSS y sistemas C-UAS LSS disponibles en el marco del proyecto CONDOR, con el objetivo de corroborar tanto las capacidades de defensa de las unidades que se determinen, como los enfoques diferentes de integración de la capacidad en PF y DA para contrarrestar esta amenaza.

[38] Funciones que realiza el Sistema de Observación y Prospectiva Tecnológica de la DGAM: vigilancia y prospectiva tecnológica, identificando las tendencias, avances y retos tecnológicos futuros.

(INTENCIONADAMENTE EN BLANCO)

ANEXO A

BIBLIOGRAFIA

NORMATIVA NACIONAL

A. Ley Orgánica 5/2005, de 17 de noviembre de la Defensa Nacional.

B. Ley 21/2003, de 7 de julio, de Seguridad Aérea.

C. Ley 8/1975, de 12 de marzo, de zonas e instalaciones de interés para la Defensa Nacional.

D. Orden Ministerial 86/2012, de 4 de diciembre, por la que se crean el Mando de Vigilancia y Seguridad Marítima y el Mando de Defensa y Operaciones Aéreas.

E. Real Decreto 601/2016, de 2 de diciembre, por el que se aprueba el Reglamento de la Circulación Aérea Operativa (RCAO).

F. Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea.

BIBLIOGRAFÍA DE ÁMBITO NACIONAL

A. CCDC. “Análisis Base”. Concepto Nacional C-UAS LSS. Madrid, 16 de julio de 2018.

B. CCDC. “Documento Grupo de Trabajo de Tecnología”. Concepto Nacional C-UAS LSS. Madrid, 6 de junio de 2018.

C. CCDC. “Informe Experimentación”. Concepto Nacional C-UAS LSS. Madrid, 10 de diciembre de 2018.

D. CESEDEN. Cte. ET. Arturo Teruel Valle. Monografía XVII CEMFAS “Capacidades de las FAS para responder a la amenaza de los drones”. Madrid, 28 de abril de 2016.

E. CESEDEN. Cte. Julio Suarez Carrasco. Monografía XVII CEMFAS “Empleo de RPAS por insurgencias y grupos terroristas. Reto para la defensa de las bases militares”. Madrid, 1 de mayo de 2016.

F. DGAM. Sistema de Observación y Prospectiva Tecnológica, SDG PLATIN “Objetivo de I+D+I relacionados con la capacitación tecnológica nacional en el ámbito de los sistemas anti-RPAS”. Madrid, 28 de junio de 2017.

G. DGAM. SDG PLATIN. “Documento de necesidad funcional Proyecto CONDOR”. Madrid, Enero 2018.

H. Estrategia de Seguridad Nacional 2017. Presidencia del Gobierno de España. Madrid, 2017.

I. IEEE. Cesáreo Gutiérrez Espada, Documento de Investigación 19/2018 “El desarrollo de un concepto conjunto de defensa contra sistemas aéreos no tripulados (C-UAS) a la luz

del Derecho Internacional de la Responsabilidad". Estudio colaboración IEEE concepto C-UAS. Septiembre 2018.

J. IEEE. Eugenia López-Jacoiste, Documento de Investigación 10/2018 "Drones armados y el Derecho internacional humanitario". Estudio colaboración IEEE concepto C-UAS. Septiembre 2018.

A. IEEE. José Alberto Marín Delgado, Documento marco 03/2018 "El uso de drones comerciales como vectores terroristas". Madrid, 29 de enero de 2018.

B. IEEE. Juan A. Moliner González, Documento opinión 16/2018 "Algunos problemas éticos de las tecnologías militares emergentes". Madrid, 19 de febrero de 2018.

C. IEEE. María José Cervell Hortal, Documento de Investigación 11/2018 "La defensa contra sistemas aéreos no tripulados (C-UAS): Una reflexión jurídica preliminar desde el punto de vista del uso de la fuerza". Estudio colaboración IEEE concepto C-UAS. Septiembre 2018.

D. JEMA. Instrucción General 00-1 "Doctrina Aeroespacial Básica". 1ª Rev. Madrid. 29/11/2018.

E. JEMAD. "Concepto de Empleo de las Fuerzas Armadas" 2017, cambio 2. Madrid, 30 de mayo de 2018.

F. JEMAD. "Directiva de Desarrollo Conceptual 01/2018". Concepto Contra-UAS. Madrid, 9 de marzo de 2018.

G. JEMAD. PDC-01 (A). "Doctrina para el empleo de las Fuerzas Armadas". Madrid, 27 de febrero 2018.

H. JEMAD. PDC-3.14 (A). "Protección de la Fuerza" (borrador). Madrid, NOV 2018.

I. MADOC ET. DIDOM-IV-017, "Tendencias 2016-2017, Volumen I, Aspectos generales". Granada, diciembre 2017.

J. MADOC ET. PD3-311, Publicación Doctrinal "Defensa Antiaérea", Granada, 9 de enero de 2015.

K. MADOC ET. PD4-300, "Empleo de la Artillería Antiaérea, Tomo I, Clasificación y tendencias de la amenaza". Granada, 6 de octubre de 2016

L. Ministerio de Fomento. Gobierno de España. "Plan Estratégico para el desarrollo del sector civil de drones en España 2018-2021". Madrid, abril 2018.

M. Ministerio del Interior. Gobierno de España. Gabinete de Coordinación y Estudios de la Secretaría de Estado de Seguridad. "Informe Grupo de Trabajo sobre Drones". Madrid, 14 de julio de 2015.

N. Presidencia del Gobierno de España. "Estrategia de Seguridad Nacional 2017. Un proyecto compartido de todos y para todos". Madrid, 2017.

DE ÁMBITO INTERNACIONAL

A. **DEU.** Presentación *COL (A) Klaus-Peter Kiser. Army Concepts and Capabilities Development Center, "Incorporating a modular C-UAS approach for the German Army". London, 18th April 2018.*

B. **DEU.** Presentación *Cap. Biel. Army Concepts and Capabilities Development Center, "Unmanned Aerial Systems (UAS) and Counter-UAS". Warminster, 25-27 April 2017.*

C. **EU.** *"EUROPEAN DRONES OUTLOOK STUDY Unlocking the value for Europe" - (SESAR Joint Undertaking), November 2016.*

D. **FRA.** *"Etude exploratoire sur la lutte anti-drone", RFT DSA 3.2. Direction des études et de la prospective artillerie (DEPA). École d'artillerie, June 2016.*

E. **FRA.** Presentación *COL (AF) Christophe Michel. State protection and security directorate, SGDSN. "French point of view on Counter-UAV. How to balance regulations with counter-drone capability". London, 19th April 2018.*

F. **FRA.** *Presentación LTC de LA BERNARDIE. DEPA/BES. Directorate for artillery studies and development. "C-UAS conceptual framework and trajectory for development".*

G. **FRA.** *Presentación LTC de LA BERNARDIE. DEPA/BES. Écoles Militaires de Draguignan. "Lutte anti-drone : Enjeux et Perspectives".*

H. Informes de los OFENs del MADOC en Alemania, Estados Unidos, Francia, Italia y Reino Unido.

I. Informe del OFEN del CCDC en US JS J7 (Suffolk).

J. **ITA**. Presentación C-UAS. Visita al *Centre for Defence Innovation Centro Innovazione della Difesa (CID).* Roma, 09 mayo 2018.

K. **ITA.** Presentación *Stato Maggiore dell'Esercito, "Unmanned Aerial Systems (UAS) and Counter-UAS". Warminster, 26th April 2017.*

L. **MCDC.** *"Counter Unmanned Autonomous Systems (CUAxS)", Project led by NATO Headquarters Supreme Allied Commander Transformation (NATO HQ SACT). 24 March 2017.*

M. **NATO.** *AJP-3.14. Allied Joint Doctrine for Force Protection. Edition A Version 1.*

N. **NATO.** *Allied Administrative Publication (AAP-06), NATO Glossary of Terms and Definitions, 2018.*

O. **NATO.** *CIED CoE. Report 1/2017 "Use of Unmanned Aerial Systems (UAS) by non-state actors", 26 April 2017.*

P. **NATO.** *Industrial Advisory Group (NIAG). Study Group 200. "Low, Slow and Small threat effectors study. Final Study Report". NAC. 06 November 2017.*

Q. **NATO.** *Industrial Advisory Group (NIAG). NATO Army Armaments Group (NAAG). Joint Capability Group on Ground Based Air Defence (GBAD). "Final Report of NIAG SG170 on engagements of Low, Slow and Small aerial targets by GBAD". NAC. 16 September 2013.*

R. **NATO.** *Industrial Advisory Group (NIAG). NATO Army Armaments Group (NAAG). Joint Capability Group on Ground Based Air Defence (GBAD). "Final Report of NIAG SG188 Study on sensor mix optimization study for emerging threats". 19 June 2015.*

S. **NATO.** *Science Technology Organization. STO-MP-SET-241. "Reconnaissance of LSS-UAS with Focus on EO-Sensors". Hans-Wilhelm Warnke.*

T. **NATO.** *Joint Air Power Competence Centre (JAPCC). "The implications for force protection practitioners of having to counter unmanned systems – a think piece". 20180623-Unclas-FP_Implications_C-US_Think-Piece-FP&DAT-V2.8.*

U. **NATO.** *ACT "NATO Strategic Foresight Analysis 2017 Report", Norfolk. 2018.*

V. **UK.** *Joint Doctrine Publication-0-30.2 "Unmanned Aircraft Systems". Development, Concepts and Doctrine Centre (DCDC). UK Ministry of Defence. Shrivenham. August 2017*.

W. **UK.** *Joint Doctrine Note 2/11 "The UK Approach to Unmanned Aircraft Systems". Development, Concepts and Doctrine Centre (DCDC). UK Ministry of Defence. Shrivenham. 30 March 2011*.

X. **UK**. *Tri Service Advice Note 01/17. Commanders of the 3 Warfare Centres. "Counter Unmanned Air Systems. Prepare the Force". 9 September 2017.*

Y. **UK.** *Doctrine Note 16/03. "OPSEC and Countersurveillance". Directorate Land Warfare, Headquarters Field Army. UK Ministry of Defence. Shrivenham. 25 July 2016.*

Z. **UK.** Presentación *COL. Giles Malec. Commander Joint Ground Based Air Defence. RAF. "C-UAS Conference". London, 18 April 2018.*

AA. **UK.** *Civil Aviation Authority. Drone Safe. "The drone code".*

BB. **US.** *Headquarters, Department of the Army. ATP 3-01.81 "Counter-Unmanned Aircraft System Techniques". 13 April 2017*.

CC. **US.** *United States "Counter-Unmanned Aircraft System (C-UAS) Strategy Extract". 5 October 2016*.

DD. **US.** *United States. Army TRADOC, Asymmetric Warfare Group. "Russian new generation warfare handbook". January 2017,*

EE. **US.** *Committee on Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations, Board on US Army Science and Technology, Division on Engineering and Physical Sciences, The National Academy of Sciences "CUAS Capability for Battalion-and-Below Operations, Abbreviated Version of a Restricted Report". Washington DC, 2018*.

FF. **US.** *The National Academies of Sciences. Study Report "Counter Unmanned Aircraft Systems (CUAS) Capability for Battalion-and-Below Operations". 2018.*

GG. **US.** Department of Defense. "Unmanned Systems Integrated Roadmap FY2013-2038".

ARTÍCULOS

A. *ADAMS, Rick. "Countering UAVs without collateral damage", Unmanned featured. Military Technology 2/2017.*

B. *ALGARA FUENTES, Luis, Tcol (ET). Academia de Artillería ET.* "Evolución de los conceptos. Del C-RAM al C-EAT".

C. *BALKAN, Serkan. SETA. "Daesh's drone strategy. technology and the rise of innovative terrorism". 2017.*

D. *BERNARDI, Beatrice, Jane's Defence Weekly. "Xponential 2017: Interagency communication, policy co-ordination needed for C-UAS". Dallas, Texas, 11-May-2017.*

E. BURGOS, Mateo. "Estado del arte de las tecnologías antidrón". Cátedra Isdefe-UPM, Observatorio tecnológico en Defensa y Seguridad. Junio 2018.

F. *BUSCH, Michel, Maj (DEU Army). JAPCC. Journal Edition 25. "Unmanned Aerial Systems miniaturization. Chances and risks of an irreversible trend". 2018.*

G. CABELLO RODRIGUEZ, José Luis. "Vehículos aéreos sin piloto. Una aproximación táctica. Escenarios y entornos de actuación". Junio 2018.

H. *MARTIN, Guy. DefenceReviewAsia. "Attacking the killer drones: counter-UAV systems". JULY/AUG 2017.*

I. *MCDONALD, Jack. International Security Department. Chatham House, the Royal Institute of International Affairs. "Drones and the European Union: Prospects for a Common Future". February 2018.*

J. *PISTOIA, Daniela. JAPCC. Journal edition 25. "Detecting and neutralizing mini-drones. Sensors and effectors against an asymmetric threat". 2018.*

K. *RASSLER, Don, United States Military Academy. "Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology".*

L. *Remote Control Project. Oxford Research Group. "The hostile use of drones by non-state actors against British targets", January 2016.*

M. *TORBJORN MOE, Knut, JAPCC. Journal Edition 21. "Small drones. From cheap toys to terrorist tools-detection and disruption challenges". 2015.*

N. VV.AA. *Proliferated Drones. "Drone Proliferation and the Use of Force - An Experimental Approach". 3/3/2017.*

O. VV.AA. *Forum / Countering the Small Unmanned Aircraft System. "The Rise of the Commercial Threat Countering the Small Unmanned Aircraft System". 2nd Quarter 2017.*

ENLACES DE INTERÉS

- http://www.arcic.army.mil/Home
- https://ctc.usma.edu/
- https://drones.enaire.es/
- https://www.fomento.gob.es/
- https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre
- http://www.horizontesdefensayseguridad.net/
- https://www.japcc.org/
- https://www.seguridadaerea.gob.es/lang_castellano/home.aspx
- https://www.sto.nato.int/Pages/default.aspx

[INTENCIONADAMENTE EN BLANCO]

ANEXO B

GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

01. La terminología empleada en la documentación analizada puede inducir a errores tanto en la propia definición de los vehículos aéreos no tripulados, como en la clasificación de éstos. En el "Anexo B", se incluyen las definiciones de los términos empleados en el concepto.

02. El propio **Reglamento de la Circulación Operativa** (RCAO) establece que "*a efectos de RCAO se considera que son sinónimos de UAV, las palabras «drone» y «vehículo aéreo pilotado remotamente» (RPA).*"[1]

03. Sin embargo, el término de UAV (*Unmanned Aerial Vehicle*) ha venido siendo interpretado por la **comunidad internacional** como las aeronaves que vuelan sin un piloto a bordo y que pueden ser pilotadas por control remoto (RPA), o bien estar programadas y ser completamente autónomas, aeronaves autónomas en terminología de la Organización Internacional de Aviación Civil (OACI)[2]. Por lo tanto, el término UAS (*Unmanned Aerial System*) incluye tanto a los RPAS (*Remotely Piloted Aircraft System*) como a los sistemas de aeronaves autónomas.

Terminología.

TERMINO	DESCRIPCIÓN	REFERENCIA
Aeronave Pilotada Remotamente (RPA)	Una aeronave que, aunque no lleva un operador humano, es volada remotamente por un piloto, es normalmente recuperable y puede llevar una carga letal o no.	JDP-0-30.2. UK
Amenaza	Toda circunstancia real, que ponga en peligro la seguridad.	PDC 01(A). ESP
Capacidad militar	Conjunto de sistemas que, operados bajo unos principios y procedimientos doctrinales establecidos, permiten obtener determinados efectos mediante su empleo en operaciones para cumplir con las misiones asignadas.	PDC 01(A). ESP
Dron	Aeronave no tripulada.	RAE. ESP
Defensa Aérea (DA)	Las operaciones de defensa aérea persiguen alcanzar el nivel apropiado de control de la situación aérea y, por tanto, la protección de la fuerza y de los puntos vitales y zonas que por su importancia estratégica u operacional se señalen	PD3-311. ESP

[1] Real Decreto 601/2016, de 2 de diciembre, por el que se aprueba el Reglamento de la Circulación Aérea Operativa. BOE núm. 292, 3 de diciembre de 2016, Pág. 84794.

[2] Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea. Pág. 129609.

Enjambre (*swarm*)	Un grupo de UAS LSS que emplean la cantidad como medio para saturar la capacidad de respuesta o la colaboración entre ellos para lograr un objetivo común.	*NIAG. Study Group 200. NATO*
Estación de control del UAS	Todos los dispositivos o elementos del sistema aéreo no tripulado desde los que se controla, monitoriza y pilota remotamente el UAV durante todas las fases del vuelo, a través de los sistemas de comunicaciones. A efectos de RCAO se considera que son sinónimos de Estación de Control, las palabras «GCS» (*Ground Control Station*) y «RPS» (*Remote Pilot station*).	RCAO. ESP
Geofencing	Técnica que emplea tecnología de posicionamiento por satélite e identificación por radiofrecuencia, con el fin de generar zonas de acceso limitado a UAS.	
Niveles de autonomía	**Control remoto LOS** (línea de visión)**.** Un operador controla todas las operaciones del UAS. El operador o un observador cercano, debe tener una línea de visión clara con el UAS para saber su localización y orientación mientras controla sus movimientos. **Control remoto sin LOS**. Un operador controla todas las operaciones del UAS sin necesidad de tener línea de visión con el UAS, ya que conoce su localización y orientación gracias a la información proporcionado por los sensores embarcados. **Semi-autónomo.** El UAS puede realizar actividades de control muy limitadas en ayuda al manejo del operador, como por ejemplo hacer estacionario y evitar obstáculos. El enlace de comunicaciones sigue siendo necesario. **Casi total autonomía**. El UAS puede realizar numerosas actividades automáticas, como control de vuelo automático (incluyendo evitar obstáculos), control de potencia (incluyendo estacionario), reconocimiento y seguimiento de objetivos. Sin embargo, Estas funciones automáticas son activadas y desactivadas por el operador, que puede supervisarlas durante la realización de la misión por parte de uno o múltiples UAS. **Totalmente Autónomo.** Uno o gran número de UAS que no requieren la intervención humana para realizar tareas complejas, como por ejemplo planear y ejecutar misiones, navegación sin señal GPS, evitar obstáculos, etc. El operador asignará las misiones y ocasionalmente supervisará la ejecución de estas.	*CUAS Capability for Battalion-and-Below Operations, Abbreviated Version of a Restricted Report*. US.
Operador de sistemas aéreos no tripulados (DUO)	Es aquella persona designada específicamente para operar remotamente los controles y mandos de vuelo de una aeronave no tripulada, ejecutando la misión programada con las adecuadas garantías de seguridad y eficacia operativa. Con la consideración de piloto al mando y comandante de aeronave se le atribuyen las responsabilidades inherentes y específicas para este puesto recogidas en el RCAO.	RCAO. ESP

Protección de la Fuerza (PF)	La Protección de la Fuerza engloba aquellas actividades que tienen como objeto minimizar la vulnerabilidad del personal, equipo, material, instalaciones, información, operaciones y actividades de la Fuerza y de los elementos no militares que apoyan, acompañan o están bajo responsabilidad de la Fuerza, frente a las acciones adversarias, propias, y frente a los riesgos sanitarios, naturales, tecnológicos y accidentes. Su finalidad es preservar la libertad de acción del Comandante y garantizar la operatividad de la Fuerza.	PDC-3.14(A) Borrador NOV 2018. ESP
Sistema aéreo no tripulado (UAS)	Aeronave y sus elementos asociados, la cual es operada sin piloto a bordo. Comprende los elementos individuales del UAS, que incluyen el vehículo aéreo no tripulado (UAV), la estación de control y cualquier otro elemento necesario para permitir el vuelo, tales como el enlace de comunicaciones o el sistema de lanzamiento y recuperación.	RCAO. ESP
Sistema Aéreo Remotamente Pilotado (RPAS)	La suma de los componentes requeridos para proporcionar la capacidad total e incluye el piloto, los operadores de sensores (si procede), aeronave pilotada remotamente, estación de control de tierra, sistemas de ayuda y de apoyo asociados, enlaces de comunicaciones por satélite y enlaces de datos.	JDP-0-30.2. UK
Sistema automático	Un Sistema automático o automatizado es uno que, en respuesta a las entradas de uno o más sensores, está programado para seguir de manera lógica un conjunto predefinido de reglas para proporcionar un resultado. Conociendo el conjunto de reglas bajo las que opera, el resultado es predecible.	JDP-0-30.2. UK
Sistema autónomo	Sistema capaz de comprender mayor nivel de intención y dirección. De esta comprensión y de su percepción del entorno, dicho sistema es capaz de tomar las acciones para lograr un estado deseado. Es capaz de decidir una línea de acción de entre una serie de alternativas, sin depender de la supervisión y el control humano, aunque éste puede seguir presente. Aunque la actividad general de un UAV será predecible, las acciones individuales pueden no serlo.	JDP-0-30.2 UK
Vehículo aéreo no tripulado (UAV)	Vehículo aéreo propulsado que no lleva personal como operador a bordo. Los vehículos aéreos no tripulados incluyen solo aquellos vehículos controlables en los tres ejes. Además, un UAV: - Es capaz de mantenerse en vuelo por medios aerodinámicos. - Es pilotado de forma remota o incluye un programa de vuelo automático. - Es reutilizable. - No está clasificado como un blanco aéreo, un arma guiada o un dispositivo similar de un solo uso diseñado para el lanzamiento de armas.	RCAO. ESP

Acrónimos.

CCDC	Centro Conjunto de Desarrollo de Conceptos
CDAG	*Concept Development Assessment Game*
CD&E	Desarrollo de Conceptos y Experimentación (*Concept Development & Experimentation*)
CEFAS	Concepto de Empleo de las Fuerzas Armadas
CENCIED	Célula Nacional Contra IED
CETSE	Centro Tecnológico de Seguridad
CICDE	*Centre Interarmées de Concepts, de Doctrines et d'Expérimentations*
CID	*Centro Innovazione della Difesa*
CIFAS	Centro de Inteligencia de las FAS
COE	Consecuencias de Empeño
COI	Consecuencias de Interceptación
C-UAS	Contra UAS
C2	Mando y control (*Command and Control*)
DA	Defensa Aérea
DAA	Defensa Antiaérea
DDC	Directiva de Desarrollo Conceptual
DGAM	Dirección General de Armamento y Material
DIGENPER	Dirección General de Personal
EA	Ejército del Aire
EMACON	Estado Mayor Conjunto
EMAD	Estado Mayor de la Defensa
ET	Ejército de Tierra
FAS	Fuerzas Armadas
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
GABTEC	Gabinete Técnico
GCS	Estación de Control en Tierra (*Ground Control Station*)
GBAD	*Ground Based Air Defence*
GPS	Sistema de Posicionamiento Global (*Global Positioning System*)
GT	Grupo de Trabajo
IEEE	Instituto Español de Estudios Estratégicos

IED	Artefactos explosivos improvisados (*Improvised Explosive Devices)*
ISDEFE	Ingeniería de Sistemas para la Defensa de España
IWD	Artefactos armados improvisados (*Improvised Weapon Devices)*
HVE	*High Visibility Event*
I+A	Instrucción y Adiestramiento
ITM	Instituto Tecnológico la Marañosa
JEMAD	Jefe de Estado Mayor de la Defensa
LOS	Línea de Visión (*Line Of Sight*)
LSS	De pequeño tamaño, a baja altura y velocidad (*Low, Slow, Small)*
MADOC	Mando de Doctrina
MALOG	Mando de Apoyo Logístico
MDOA	Mando de Defensa y Operaciones Aéreas
MINISDEF	Ministerio de Defensa
MIRADO-I	Material, Infraestructura, Recursos Humanos, Adiestramiento Doctrina, Organización e Interoperabilidad
MOPS	Mando de Operaciones
OFEN	Oficial de Enlace
OTAN	Organización del Tratado del Atlántico Norte
PDC	Publicación de Doctrina Conjunta
PF	Protección de la Fuerza
PMO	Problema Militar Operativo
RAP	Situación aérea evaluada (*Recognized Air Picture*)
RCAO	Reglamento de Circulación Aérea Operativa
ROE	Reglas de enfrentamiento (*Rules Of Engagement*)
ROV	Redes de Observadores Visuales
RPS	Estación de Control Remoto (*Remote Pilot Station*)
SBAD	Defensa Aérea Basada en Superficie (*Surface Based Air Defence*)
SDG PLATIN	Subdirección General de Planificación Tecnología e Innovación
SES	Secretaría de Estado de Seguridad
SICADA	Sistema de Captura de Datos
TN	Territorio Nacional
TTP	Tácticas, Técnicas y Procedimientos

UAS	Sistemas aéreos no tripulados (*Unmanned Aerial Systems)*
UNED	Universidad Nacional de Educación a Distancia
UE	Unión Europea

ANEXO C

ESCENARIOS, ENTORNOS Y TIPOS DE PROTECCIÓN

01. De acuerdo con el Concepto de Empleo de la Fuerzas Armadas (CEFAS), se establecen **tres escenarios generales** donde las FAS deberán desarrollar su labor[1]:

    a. **Seguridad del territorio nacional**, en el que las FAS actúan fundamentalmente mediante la disuasión, la prevención y la vigilancia permanente de sus espacios de soberanía, y llegado el caso, con su defensa militar.

    b. **Seguridad exterior**, derivado de nuestros compromisos en el contexto multinacional, multilateral o bilateral y de la protección de los intereses de España en el exterior.

    c. **Seguridad nacional ampliada**, en el que las FAS proporcionan bien una respuesta específica, o bien contribuyen a una respuesta general como parte de la Acción del Estado.

02. Por otra parte, dentro de cada uno estos escenarios se distinguen **dos entornos** diferentes: **abiertos** y **urbanos**. Los entornos urbanos presentan dificultades añadidas para la detección, seguimiento, identificación y neutralización de UAS LSS, así como una serie de implicaciones para tener en cuenta:

    - Eventos de afluencia masiva de ciudadanos (conciertos, manifestaciones, competiciones deportivas, etc.).
    - Proximidad de zonas de vuelo de otras aeronaves (aeropuertos y helipuertos).
    - Áreas de seguridad especial (infraestructuras críticas, edificios gubernamentales, etc.).
    - Nodos estratégicos de telecomunicaciones.
    - Áreas de alta densidad electromagnética.

03. Asimismo, es preciso diferenciar **tres tipos de protección** a la hora de proporcionar defensa C-UAS LSS a un objetivo determinado, que a la vez están relacionadas con los tres escenarios generales de actuación (seguridad del territorio nacional, seguridad exterior y seguridad nacional ampliada) y los dos entornos (abierto y urbano):

    a. **Protección permanente de un objetivo estático**, como bases militares (terrestres, navales y aéreas), aeropuertos, infraestructuras críticas (centrales nucleares, centros de comunicaciones, etc.), instalaciones de interés (edificios gubernamentales, etc.).

    b. **Protección temporal de un objetivo estático**, como eventos de alta visibilidad (*High Visibility Events*, HVE), competiciones deportivas, conciertos, cumbres políticas, etc.

    c. **Protección temporal de un objetivo móvil**, como un convoy militar, vehículos de personalidades, movimientos de tropas, etc.

[1] EMAD. "Concepto de Empleo de las Fuerzas Armadas 2017", cambio 2. Madrid, 30 mayo 2018. Pág. 23.

[INTENCIONADAMENTE EN BLANCO]

ANEXO D

METODOLOGÍA EMPLEADA

1. FASE DE INVESTIGACIÓN.

01. El propósito de la fase de Investigación ha sido recabar el conocimiento explícito existente en la organización sobre el problema, la solución actualmente en uso y las posibles soluciones alternativas, así como identificar en qué áreas no existe conocimiento documentado que deba ser descubierto o desarrollado en el seno del Grupo de Expertos en las posteriores fases del proyecto. El análisis se ha realizado tanto a nivel nacional como de los principales países del entorno y organizaciones internacionales, mediante dos procesos:

- Análisis Bibliográfico. Investigación y análisis de la documentación existente sobre el problema para mejorar su comprensión y enfocar la tesis de la solución.
- Análisis de los *Stakeholders*. Investigación sobre las partes de la organización que están en contacto con el problema, quién puede ayudar a resolverlo, y quién está involucrado en la implantación de la solución.

02. El producto de la fase de investigación fue el informe del **Análisis Base** o "*Baseline Assessment*", para el que se han llevado a cabo las siguientes acciones:

- Revisión y análisis de documentos nacionales e internacionales, los más relevantes se incluyen en el "Anexo A".
- Creación de un Grupo de Trabajo (GT) de Tecnología, formado por expertos del Sistema de Observación de Prospectiva y Tecnología de la SDG PLATIN DGAM, CIFAS y MOPS-J2, para realizar un estudio prospectivo sobre nuevas tecnologías y posibilidades en la defensa C-UAS, aprovechando los trabajos realizados en el contexto del "Proyecto CONDOR" C-RPAS.
- Creación de un GT de Industria, formado por expertos de las principales empresas nacionales[1] involucradas en el desarrollo de sistemas C-UAS, que han proporcionado información sobre sus sistemas y que participarán en las siguientes fases del proyecto.
- Creación de un GT de Academia, formado por profesores de Universidades[2] y expertos del Instituto Español de Estudios Estratégicos (IEEE), para realizar un estudio académico sobre temas relacionados con las implicaciones legales y éticas de la defensa C-UAS, estado del arte de tecnologías y escenarios de actuación.

[1] CENTUM, INDRA, ART Radar, Thales España, Escribano *Mechanical & Engineering*, IECISA. Listado proporcionado por la SDG INREID DGAM, Oficio DGAM S-18-013854, de 16/05/2018.
[2] Facultad de Derecho de las Universidades de Murcia y Navarra, Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid.

- Solicitada una Petición de Información a los Oficiales de Enlace (OFEN) del Mando de Adiestramiento y Doctrina (MADOC) del ET en Alemania, Estados Unidos, Francia, Italia y Reino Unido, para que proporcionasen información actualizada sobre cómo tienen implementada la capacidad C-UAS en estos países, o los desarrollos conceptuales en caso de no disponer de la citada capacidad. Asimismo, se ha recibido información del OFEN del CCDC el *US Joint Staff J7* (*Suffolk*).
- Consultas con expertos del CENCIED, Academia de Artillería del ET, MALOG ET, ITM la Marañosa, SDG PLATIN DGAM, Guardia Civil, Policía Nacional, así como de Alemania, Estados Unidos, Francia, Holanda, Italia y Reino Unido.
- Reuniones con los OFEN francés y alemán en el EMACON. Asimismo, se han establecido contactos y se ha recibido información del *Centro Innovazione della Difesa* de Italia (CID, Roma) y del *Centre Interarmées de Concepts, de Doctrines et d'Expérimentations* de Francia (CICDE, París).
- Establecidos contactos con la Secretaria de Estado de Seguridad (SES) y mantenido una reunión con el Jefe de Servicio del Área de Seguridad Ciudadana y Operaciones del Gabinete de Coordinación y Estudios, y con personal del Área de Normativa del Gabinete de Coordinación y Estudios, para coordinación con los trabajos desarrollados por el Grupo de Trabajo Interministerial de Drones (JUN 18).
- Asistencia a diferentes conferencias y cursos: al V Congreso I+D en Seguridad y Defensa (Toledo, 22-24 NOV 17); a la Jornada Tecnológica Anti-dron del CETSE (El Pardo, 15 MAR 18); a la Conferencia Anual Internacional *Counter-UAS* (Londres, 17-19 ABR 18); al Curso *NATO CD&E* (*Oberammergau*, 07-11 MAY 18); a la Cumbre Europea UNVEX en Seguridad y Defensa (León, 29-31 MAY 18); a las pruebas de sistemas C-UAS portátiles del Proyecto "CONDOR" (ITM la Marañosa, 20 JUN 18); al Curso de verano de la UNED "Los drones: una amenaza o una oportunidad" (Madrid, 02-04 JUL 18); a la Jornada Tecnológica Secudron en el ITM (San Martín de la Vega, 04 OCT 18); al *Workshop on Countering Terrorist Misuse of UAS* (Bruselas, 09-10 OCT 18); al VI Congreso I+D en Seguridad y Defensa (Valladolid, 20-22 NOV 18).
- Creación y empleo del portal "Concepto Nacional Contra UAS" en la aplicación SICADA (SIstema de CAptura de DAtos) diseñada por el INTA para el CCDC, accesible desde internet mediante usuario registrado y contraseña (https://sicada.inta.es/sicada/). Durante la fase de Investigación, la aplicación se empleó para compartir información entre los expertos que participan en el proyecto. En la siguiente fase de Descubrimiento y Desarrollo se empleará como foro de discusión de los temas de estudio y para realizar cuestionarios, que nos permitirán la recogida automática de datos para el posterior análisis.

03. Durante la investigación se han identificado una serie de "**hallazgos**", entendidos como piezas de información referenciadas a un documento, que contribuyen a definir el problema o el modelo investigado. Estos hallazgos se han almacenado en una tabla en forma de fichas bibliográficas, agrupadas por temas de estudio para facilitar su referencia.

2. FASE DE DESCUBRIMIENTO Y DESARROLLO.

04. **Diseño de la fase de descubrimiento.** Durante la fase de descubrimiento se empleó una metodología mixta basada en cuestionarios estructurados y cerrados complementada con recogida de información semi-estructurada mediante grupos de discusión.

05. **Muestra.** Se contó con una muestra de 23 participantes de los distintos agentes de información considerados *Ministerio de Defensa*, *Secretaria de Estado de Seguridad* (SES), *Academia* e *Industria*, que participaron en distinta medida en cada una de las fases. Respecto al Ministerio de Defensa se contó con 12 representantes en total (ARMADA, CENCIED, CIFAS, DIGENPER, DGAM, EA, EMACON, ET y MOPS), siendo 2 los representantes del Ejército de Tierra, del Aire y del DGAM. Se contó con 2 representantes de la SES. Respecto de *Academia* se contó con 3 representantes (IEEE, Universidad de Murcia y Universidad Politécnica de Madrid), principalmente para atender a los aspectos legales. Por último, se contó con 6 representantes de la *Industria* (ART Radar, Centum, Escribano, IECISA, Indra y Thales).

06. **Medida de *expertise*.** En primer lugar, se solicitó a los 23 expertos que rellenaran un breve cuestionario para tener una medida de su conocimiento y experiencia previa en el campo de estudio (*expertise*). Dicha medida permite eventualmente ponderar los resultados dando un mayor peso cuanto mayor es la experiencia y conocimiento del participante. Concretamente, se pidió que indicarán el grado de conocimiento del área, las fuentes de dicho conocimiento, su experiencia previa y el grado esperado de convergencia-divergencia de su conocimiento respecto del resto de participantes.

07. **Cuestionario semiestructurado.** En segundo lugar, se procedió a una recogida semiestructurada de información con objeto de alcanzar la exhaustividad de conceptos sobre el tema de estudio. En esta fase participaron 12 representantes del Ministerio de Defensa y de la SES: ARMADA, CENCIED, CIFAS, DGAM, EA, ET, MOPS y SES (con dos representantes de cada uno de los Ejércitos); dos representantes de *Academia* (Universidad de Murcia y Universidad Politécnica de Madrid) y los 6 representantes de *Industria*.

08. Partiendo del **enfoque MIRADO-I** se plantearon preguntas abiertas en relación a dos escenarios de defensa, el empleo hostil de sistemas no tripulados de pequeño tamaño contra unidades e instalaciones militares en operaciones fuera y dentro del territorio nacional. Específicamente se pidió a los participantes que generaran una lista de aspectos relevantes en cada uno de los escenarios buscando exhaustividad y relevancia.

09. La información procedente de esta recogida de datos se analizó mediante **técnicas de análisis temático** de contenidos en el programa “Atlas.ti 8”. Dos evaluadores entrenados leyeron el material varias veces para extraer códigos de manera independiente. Posteriormente los dos evaluadores, junto con un tercero, discutieron y acordaron la lista definitiva de códigos. Por último, se llevó a cabo la codificación de todo el material mediante los códigos generados. Tras dicha codificación se analizó la relevancia de los conceptos que emergieron con base a su frecuencia de aparición y coocurrencia. Se prestó especialmente atención al grado de acuerdo entre los conceptos aparecidos y su aparición en el Análisis Base, así como a la relevancia relativa atribuida en cada caso. Se generaron 107 códigos, encontrándose un elevado grado de solapamiento con los conceptos del

Análisis Base (65%) y una proporción media de conceptos nuevos (35%). Estos datos se tomaron como indicativos de la bondad del método. Se identificaron 7 temáticas que presentaban discrepancias tanto entre los distintos interlocutores como entre los interlocutores y el Análisis Base. Estas temáticas fueron seleccionadas como temas de discusión para el trabajo en grupo.

- Tema 1. Fundamentos doctrinales: Defensa Aérea o Protección de la Fuerza
- Tema 2. Integración de los sistemas C-UAS
- Tema 3. Personal y Adiestramiento: grado de especialización
- Tema 4. Nivel de automatización de los sistemas C-UAS
- Tema 5. Creación de un Centro de Coordinación C-UAS
- Tema 6. Importancia relativa de las fases de operación en cada escenario
- Tema 7. Evaluación de despliegues de los C-UAS

10. **Grupo de discusión.** Con objeto de recabar argumentos que apoyasen cada una de las posturas encontradas, se trabajó con las 6 primeras temáticas en grupos presenciales mediante un contexto estructurado. En esta fase se trabajó en grupo solo con los expertos correspondientes al Ministerio de Defensa y a la SES. En esta fase participaron los expertos de ARMADA, CENCIED, CIFAS, DGAM, EA, EMACON, ET, MOPS y SES. Se realizaron dos sesiones de 4h de duración cada una, tratándose tres temáticas por sesión.

11. Los temas fueron debatidos uno a uno bajo el siguiente **formato de discusión** que se desarrolló de forma consecutiva:

- **Exposición del tema.** Se expuso la dimensión relevante mostrando argumentos a favor y en contra de las distintas opciones de entre los extraídos del cuestionario semiestructurado.
- **Ronda de intervenciones.** Se pidió a cada participante que expresase su punto de vista sobre la cuestión. Se permitió a cada participante dos intervenciones, siempre en orden previamente aleatorizado y sin dar posibilidad de réplica más allá del turno.
- **Valoración de opciones.** Los participantes puntuaron cada una de las opciones en una escala Likert[3] de 1-5. La valoración de las opciones se realizó de forma oculta. Una vez respondidos los resultados medios fueron comunicados a todo el grupo.
- **Argumentación final.** Por último, se pidió a los participantes que argumentaran por escrito a favor o en contra de la opción elegida mayoritariamente. Esta se realizó también de forma oculta.

12. Durante las rondas de intervención dos observadores registraron de forma estructurada las opiniones de cada uno de los participantes. Igualmente, se guardó registro escrito de los argumentos finales a favor y en contra de la opción mayoritaria, así como de las

[3] Escala psicométrica comúnmente utilizada en cuestionarios para la investigación, en la que al responder a una pregunta se especifica el nivel de acuerdo o desacuerdo conforme a la escala establecida.

puntuaciones asignadas a cada opción. En caso de no poder asistir (los representantes de DGAM en la primera sesión y de CENCIED en la segunda) los datos de los puntos 3 y 4 se registraron mediante un cuestionario *online*. Igualmente, la última temática (nº 7) se trabajó solo de manera *online*, recabando por tanto la valoración de opciones y la argumentación final.

13. La información procedente de la valoración de las distintas opciones se analizó cuantitativamente mediante la media y la desviación típica de cada opción. Adicionalmente mediante un análisis de conglomerados se analizó el conjunto de respuestas valorando la similitud entre las respuestas de los distintos participantes con objeto de detectar la presencia de posibles grupos de opinión.

14. La información procedente tanto de la recogida de datos observacionales de las opiniones de los participantes, como de la argumentación final por escrito se analizó cualitativamente poniendo el foco en la extracción de información no considerada anteriormente en el análisis de los resultados recogidos mediante el cuestionario semiestructurado.

3. FASE DE EXPERIMENTACIÓN.

15. **Diseño.** Se diseñó un experimento del tipo CDAG (*Concept Development Assessment Game*) de acuerdo al *Handbook. V 4.1. Allied Command Transformation. Feb 2014*. Se trató de un "juego de tablero" que suple las carencias de medios y de tiempo para llevar a cabo experimentos de campo, orientado a la discusión abierta en un ambiente de libertad intelectual, pero con un enfoque sistemático propio una simulación.

16. El objetivo fue evaluar las diferencias entre los enfoques abordar la defensa C-UAS-LSS desde la capacidad de Protección de la Fuerza o la Defensa Aérea. Para ello, se diseñaron tres escenarios diferentes (1: base aérea en zona de operaciones fuera de territorio nacional, 2: buque navegando por aguas restringidas cerca de costa y 3: base terrestre en zona de operaciones fuera de territorio nacional más convoy en tránsito). Se formaron 2 grupos de planeamiento de 6 integrantes cada uno, que realizaron los planeamientos desde los dos enfoques diferentes en cada uno de los 3 escenarios.

17. En el experimento participaron un total de 26 sujetos. Cada grupo de planeamiento estuvo compuesto de 3 integrantes fijos que participaron en los 3 escenarios y de 3 participantes específicos que participaron solo en el escenario correspondiente a su *expertise* (en total 9 participantes por grupo, 3 por cada escenario). Los 3 participantes fijos, que asistieron en los 3 escenarios, eran participantes de las fases anteriores de desarrollo del concepto. En todos los casos salvo en uno estos participantes se asignaron a la condición de estudio de forma congruente con la opinión manifestada en las fases anteriores (aquellos expertos que habían defendido situar los sistemas C-UAS LSS bajo la capacidad de PF fueron asignados a la condición experimental de PF y aquellos participantes que habían defendido la situación bajo la capacidad de DA fueron asignados a la condición de DA. Los 18 restantes participantes de cada grupo (3 por cada escenario y grupo) fueron seleccionados en función del escenario, 6 participantes del Ejército del Aire para el escenario 1, 6 de la Armada para el escenario 2 y 6 del Ejército de Tierra para el escenario 3.

18. Por último, ambos grupos contaron con dos asesores externos, uno sobre aspectos legales y otro sobre aspectos metodológicos. Los asesores fueron los mismos para los dos grupos

siendo expertos en el tema de estudio y habiendo participado en las fases previas de desarrollo del concepto.

19. **Procedimiento.** Durante tres días consecutivos se llevó a cabo la situación experimental desarrollando en primer lugar el escenario aéreo, en segundo lugar el marítimo y por último el terrestre. En cada sesión se procedió de la siguiente manera.

- **Introducción y presentación del escenario** (30 minutos). Al comienzo de cada ejercicio los participantes de ambas condiciones recibieron una explicación común del escenario donde se les indicó el planeamiento a realizar, los recursos disponibles y el mapa de la situación. Se dio la instrucción de que cada grupo debía realizar un planeamiento de defensa bajo las mismas condiciones, pero orientado bien desde PF bien desde DA.

- **Desarrollo del planeamiento** (2h). Tras la explicación del escenario cada grupo fue ubicado en una sala separada contando con dos horas para la realización del planeamiento. Para dicho planeamiento los equipos tenían a su disposición un mapa del escenario y cartas representando: 1) los distintos recursos disponibles en términos de tecnología (medios de detección, identificación y afrontamiento); 2) aquellas variables relevantes identificadas durante la fase de descubrimiento del concepto (nivel de integración, automatización de los procesos o nivel de adiestramiento); 3) las posibles amenazas a afrontar. Al final de esta fase cada equipo debía rellenar un cuestionario (cuestionario 1) con las características principales de su planeamiento.

- **Afrontamiento de incidencias** (1h). Durante esta fase se diseñaron entre 4-6 incidencias en cada escenario en las que los equipos debían afrontar una posible amenaza. Por parejas los investigadores expusieron las amenazas a los participantes que debían indicar como resolvía su planeamiento dicha amenaza en términos de detección, identificación y neutralización. Mientras que un investigador definía la amenaza e interactuaba con los participantes, el otro registraba información sobre las debilidades y fortalezas de cada planeamiento.

- **Exposición y evaluación de los planeamientos** (1.5h). En una última sesión cada equipo expuso brevemente (20 minutos) su planeamiento, seguido de un turno para discutir y resolver las posibles dudas. Al final de dicha exposición cada participante rellenó de forma individual y oculta un cuestionario evaluando cada planeamiento en las variables relevantes.

20. **Variables y medidas.** Como variables del estudio se registraron las siguientes para cada planeamiento:

- Eficacia de la Defensa
- Cobertura de la Protección C-UAS
- Capacidad de Operar dentro del Tiempo de Reacción
- Probabilidad Daños Colaterales
- Grado de Interferencia en la Misión Principal

- Prevención
- Sostenimiento
- Flexibilidad
- Gestión Integral del Espacio Aéreo

21. Para la medida de estas variables, los distintos recursos ofrecidos a los equipos tenían una puntuación concreta en cada una de las variables a medir, de manera que la elección de los recursos necesarios en cada uno de los planeamientos permitía revelar diferencias en estas variables. Además, se pidió a los participantes que en determinadas características concretas (integración o adiestramiento) señalaran donde se encontraba su planeamiento (cuestionario 1).

22. Por otro lado, durante la inyección de incidencias se registraron las discusiones y opiniones emitidas sobre el funcionamiento del planeamiento, sus puntos débiles y fuertes para afrontar determinadas situaciones.

23. Finalmente, se pidió a los participantes que evaluaran de cada planeamiento su grado al final de cada sesión en una escala Likert de 5 opciones de respuesta (cuestionario 2). Se pidió información sobre las variables del estudio.

24. **Análisis de datos.** En el análisis de los datos se ha empleado estadística descriptiva por medio de medias y desviaciones típicas. Para evaluar el peso que los participantes consideraron que tenían en sus planeamientos, la condición experimental frente a los miembros concretos que componían los equipos, se empleó un ANOVA 2x3x2 teniendo en cuenta el efecto del escenario (aéreo, marítimo y terrestre) así como la condición de origen de los evaluadores.

25. De la misma manera, para comparar las puntuaciones de los planeamientos realizados desde DA o PF en cada una de las variables analizadas, se empleó una ANOVA 2x3x2, teniendo en cuenta el efecto del escenario (aéreo, marítimo y terrestre), así como la condición de origen de los evaluadores. En todo caso se trabajó con un nivel de confianza del 95% considerando significativas las diferencias con un valor de probabilidad asociado, $p < .05$.

[INTENCIONADAMENTE EN BLANCO]

ANEXO E

EQUIPO DEL PROYECTO

Dirección y equipo de apoyo.

CF. D. Ernesto GRUESO GARCÍA, CCDC, Jefe de proyecto.

CF. D. Fernando DEL POZO BERENGUER, CCDC, Dirección fase de experimentación.

CAP. ET. D. Juan José Pérez Consuegra, ITM, Asistencia técnica SICADA.

D. Daniel González Galdo, ISDEFE, Coordinador equipo de apoyo y asistencia técnica.

D. Luis Coto Sauras, ISDEFE, Equipo de apoyo.

Dª. Ana López San Román Blanco, ISDEFE, Equipo de apoyo.

D. Héctor Cuevas Esteban, Equipo de apoyo.

Dr. José Manuel Caperos Montalbán, Semantia Lab, Coordinador equipo de recogida y análisis de datos.

Dra. Diana Pérez Arechaederra, Semantia Lab, Coordinación de la recogida cualitativa de datos.

Dra. Rocío Schettini del Moral, Semantia Lab, Coordinación y formación en el análisis cualitativo.

Dr. Guillermo de Jorge y Botana, Semantia Lab, Diseño de la investigación.

Dr. Ricardo Olmos Albacete, Semantia Lab, Diseño de cuestionarios y análisis cuantitativo.

Expertos Organización.

Cte. IM. D. Francisco Antonio la Torre Morales, CENCIED, Experto.

Cor. ET. D. José Luis Sueiras Villalobos, CIFAS, Experto.

Tcol. ET. D. Jesús Molino Martínez, CIFAS, Experto.

Cte. ET. D. Francisco de Borja Olivares, CIFAS, Experto.

Cap. ET. D. Raul Gonzalez Otero, CIFAS, Experto.

Cte. GC. D. Fernando Alcázar Pérez, SES, Experto.

Tte. GC. D. Carlos Manuel Fernández González, SES, Experto.

Tcol. ET. D. Diego Villanueva Cuenca, MOPS, Experto.

Cte. ET. Dª. Elena Carretero Bravo, MOPS, Experta.

Cte. ET. D. Sergio Cobos Marquina, MOPS, Experto.

CF. D. Felix Peñuelas González, EMACON, Experto.

CF. D. David Fernández Portal, EMACON, Experto.

Tcol. EA. D. Carlos J. Ruiz Fernández, EA, Experto.

Cor. EA. D. Gonzalo Vallejo Díaz, EA, Experto.

Cte. EA. D. Abel Gómez Martos, EA, Experto.

Cap. EA. D. José Alberto Escolar Rojo, EA, Experto.

Tcol. IM. D. Miguel Hernández Suarez-Llanos, Armada, Experto.

Tcol. ET. D. Francisco Javier Rodriguez-Monteverde Cantarell, ET, Experto.

Tcol. ET. D. Luis Algara Fuentes, ET, Experto.

Tcol. ET. D. Juan Antonio Ortega Seral, DGAM, Experto.

Grupo de Trabajo de Tecnología

D. Cesar Heras Menor de Gaspar, DGAM, GT tecnología

D. Guillermo Carrera Lopez, DGAM, GT tecnología.

Dª. Yolanda Benzi Rabazas, DGAM, GT tecnología.

Dª. Rosalia Vindel Roman, DGAM, GT tecnología.

D. Pedro Carda Barrio, DGAM, GT tecnología.

D. Luis Miguel Requejo Morcillo, DGAM, GT tecnología.

Grupo de Trabajo de Academia

D. David Ramirez Morán, IEEE, Experto.

Cor. ET. D. José Luis Cabello Rodriguez, IEEE, GT Academia

Dª. María José Cervell Hortal, Facultad de Derecho Universidad de Murcia, GT Academia.

Dª. Eugenia López-Jacoíste Díaz, Universidad de Navarra, GT Academia

D. Cesareo Gutierrez Espada, Facultad de Derecho Universidad de Murcia, GT Academia

D. Marteo Burgos, Universidad Politécnica de Madrid, GT Academia

Grupo de Trabajo de Industria

D. Hector Coloma Calvo, CENTUM, GT Industria.

D. Miguel Angel Acitores Villazan, INDRA, GT Industria.

D. Vicente Pastor, ART RADAR, GT Industria.

D. Gonzalo Aréchaga Tarruell, THALES ESPAÑA, GT Industria.

D. Jose Carlos Hidalgo, EM&E, GT Industria.

D. Alejandro Villalba Centelles, IECISA, GT Industria.

Grupo de Experimentación

Cte. ET. D. Eugenio Gregorio Marín Nieto, ET, Grupo Experimento.

Cte. ET. D. Claudio Alfonso Domínguez Saucedo, ET, Grupo Experimento.

Cte. ET. D. José María Quirós Iglesias, ET, Grupo Experimento.

Cap. ET. D. Jesús Abad Sánchez, ET, Grupo Experimento.

Cap. ET. D. José Ignacio Alameda Maldonado, ET, Grupo Experimento.

Tte. ET. D. Álvaro García González, ET, Grupo Experimento.

CF. D. Carlos Carballeira, Armada, Grupo Experimento.

CC. D. Miguel Perales Garat, Armada, Grupo Experimento.

CC. D. Calvar Cerecedo, Armada, Grupo Experimento.

CC. D. Carlos Pajares, Armada, Grupo Experimento.

TN. D. Cordero de la Puente, Armada, Grupo Experimento.

Cap. IM. D. De Nicolas Martínez, Armada, Grupo Experimento.

Cte. EA. D. Humberto Antonio Briones Valero, EA, Grupo Experimento.

Cap. EA. D. José Remis González, EA, Grupo Experimento.

Cte. EA. D. Antonio Manuel Salazar Pico, EA, Grupo Experimento.

Cap. EA. D. Ramón García Jiménez, EA, Grupo Experimento.

Cte. EA. D. Jorge Díaz-Alersi Gallego, EA, Grupo Experimento.