Universidad Zaragoza
1542

Trabajo Fin de Grado

USO DE CONTRAMEDIDAS ELECTRÓNICAS EN ZONA DE OPERACIONES Y RESPONSABILIDAD DEL MANDO.

Juan Francisco Castillo Rodríguez

Director académico: Antonio Otal Germán

Director militar: Comandante Eduardo Lobo Almazán

Centro Universitario de la Defensa-Academia General Militar

2022

Agradecimientos

Primeramente, quiero agradecer al Director Académico de este Trabajo Fin de Grado, Don Antonio Otal German por la atención e interés recibido durante el desarrollo del proyecto. Gracias por las instrucciones y correcciones recibidas. Además de su dedicación, lo que ha permitido, en gran medida, la realización de este trabajo.

Del mismo modo, quiero agradecer al Director Militar, el Comandante Eduardo Lobo Almazán por su constante empeño y dedicación durante todo el periodo de prácticas. Agradecer también su esfuerzo e interés para orientarme en la Unidad de Guerra Electrónica II/31 (UEW II/31), lo que ha permitido que pudiera formar parte de la misma desde el primer día, aprendiendo y aprovechando el tiempo todo lo posible cada momento.

También quiero agradecer a todo el personal que forma la Compañía de Guerra Electrónica Ligera 1/II/31 por todo el apoyo y formación recibida, así como por fomentar un inolvidable periodo de prácticas. En especial, quiero agradecer al Teniente Jorge Robles Carpio, al Brigada Ricardo Rodríguez Baña y al Sargento Yone Armas Pérez por su disponibilidad completa para colaborar con sus conocimientos y guiarme en la realización del trabajo y de las prácticas externas.

Quiero terminar agradeciendo a mi familia y amigos por todo el apoyo recibido durante mi carrera militar, en especial, durante el periodo de formación en la Academia General Militar, sin su comprensión y apoyo constante, no hubiera podido finalizar este periodo.

RESUMEN

Durante las últimas dos décadas, la Guerra Electrónica (EW) ha ido ganando importancia en el desarrollo de las operaciones militares. Prueba de esto es que, junto a los dominios clásicos, mar, aire y tierra, se considera otro de igual o mayor importancia que los anteriores, el electromagnético. En este contexto, se encuentra la Compañía de Guerra Electrónica Ligera 1/II/31 realizando sus operaciones, siendo una unidad puntera y especializada en el empleo de medios tácticos de EW en zona de operaciones.

El desarrollo de nuevas tecnologías como la Inteligencia Artificial (IA), abre un sinfín de posibilidades, como la creación de Sistemas Autónomos de Armas (AWS). Sin embargo, la falta de consenso para la creación de una jurisprudencia específica que se adapte a la realidad de la situación y a la propia velocidad del desarrollo tecnológico genera numerosos interrogantes. Especialmente, a la hora de determinar la responsabilidad en estos nuevos sistemas de armas autónomos con capacidad para adquirir, identificar, seleccionar y realizar ataques de forma autónoma.

Para la realización del trabajo y solucionar el problema expuesto, se ha realizado un análisis documental acerca de la jurisprudencia existente, tanto nacional como internacional. También se han realizado tres encuestas a personal especializado, con experiencia en medidas de EW y que participan activamente, bien sea en la explotación de los propios sistemas EW o en el desarrollo de estos. A partir de la información recabada, se han planteado una serie de supuestos casos de estudio en los que queda patente la falta de regulación respecto a la responsabilidad del mando en el empleo de AWS.

Finalmente, se ha realizado una propuesta de regulación a nivel OTAN, que pretende ser la base sobre la que se pueda desarrollar una jurisprudencia específica que responda a los interrogantes propios del desarrollo tecnológico. Esta propuesta se ha realizado con el asesoramiento de personal con estudios jurídicos y atendiendo tanto a los problemas expuestos como a las lagunas jurídicas existentes.

PALABRAS CLAVE

Guerra electrónica, contramedida electrónica, sistema autónomo de armas, responsabilidad, jurisprudencia.

ABSTRACT

During the last two decades, Electronic Warfare (EW) has been gaining importance in the development of military operations. Proof of this is that, together with the classical domains, sea, air and land, another one of equal or greater importance is considered than the previous ones, the electromagnetic. In this context, the Light Electronic Warfare Company 1/II/31 is carrying out its operations, being a leading unit and operations specialized in the use of EW tactical means in the area of operations.

The development of new technologies such as Artificial Intelligence (AI) opens up endless possibilities, such as the creation of Autonomous Weapons Systems (AWS). However, the lack of consensus for the creation of a specific jurisprudence that adapts to the reality of the situation and the very speed of technological development raises many questions. Especially, when it comes to determining responsibility in these new autonomous weapons systems with the capacity to acquire, identify, select and carry out attacks autonomously.

In order to carry out the work and solve the exposed problem, a documentary analysis has been carried out on the existing jurisprudence, both national and international. Three surveys have also been carried out on specialized personnel, with experience in EW measures and who actively participate, either in the operation of the EW systems themselves or in their development. Based on the information collected, a series of alleged case studies have been raised in which the lack of regulation regarding command responsibility in the use of AWS is clear.

Finally, a regulation proposal has been made at the NATO level, which aims to be the basis on which a specific jurisprudence can be developed that responds to the questions inherent to technological development. This proposal has been made with the advice of personnel with legal studies and taking into account both the problems exposed and the existing legal gaps.

KEYWORDS

Electronic warfare, electronic countermeasure, autonomous weapons system, responsibility, jurisprudence.

INDICE DE CONTENIDO

AGRADECIMIENTOS ..... **I**

RESUMEN ..... **III**

ABSTRACT ..... **IV**

INDICE DE CONTENIDO ..... **V**

INDICE DE FIGURAS ..... **VII**

INDICE DE TABLAS ..... **VIII**

ABREVIATURAS, SIGLAS Y ACRÓNIMOS ..... **IX**

1. INTRODUCCIÓN **1**

2. OBJETIVOS Y METODOLOGÍA **3**

2.1. Objetivo y alcance 3

2.2. Metodología 4

2.2.1. Revisión documental 4

2.2.2. Entrevistas 4

2.2.3. Estudio de casos 5

3. ANÁLISIS DEL MARCO JURÍDICO ACTUAL **6**

3.1. Marco Legal Español 6

3.1.1. Ley Orgánica 14/2015 del Código Penal Militar. 6

3.1.2. Código Penal 7

3.1.3. Obediencia del subordinado 8

3.2. Marco Legal Internacional 8

3.2.1. Protocolo Adicional I de 1977 9

3.2.2. Derecho Consuetudinario 10

3.2.3. Estatuto de Roma de 1998 de la Corte Penal Internacional 10

3.2.4. Conflicto Armado Nacional 10

4. DETERMINACIÓN DE CAPACIDADES DE EW **11**

4.1. Medios EW 11

4.2. Medios AWS 12

5. RESPONSABILIDAD DEL MANDO EN AWS **15**

5.1. AWS y en el marco del DIH 15

5.2. Responsabilidad del mando en sistemas de armas con IA. 17

5.3. Tratamiento de responsabilidad en diversos estudios de caso. 18

5.3.1. Supuesto de escucha no autorizada. 18

5.3.2. Supuesto de error en un AWS con IA 20

5.3.3. Supuesto perturbación en el espectro electromagnético. 21

6. PROPUESTA PARA LA CREACIÓN DE REGULACIONES FUTURAS 23

6.1. Objetivos de la propuesta 23

6.2. Propuesta de regulación de AWS 23

7. CONCLUSIONES 30

REFERENCIAS BIBLIOGRÁFICAS 32

ANEXOS 34

1. ANEXO I. PLANTILLA ORGÁNICA CÍA. DE EW 1/II/31 34

2. ANEXO II ACUERDO DE CONFIDENCIALIDAD 35

3. ANEXO III MODELO DE ENTREVISTA 37

INDICE DE FIGURAS

Figura 1: Medidas de EW. Fuente: ACART-VA-005……11

Figura 2: Plantilla Orgánica. Fuente: Elaboración Propia……...34

INDICE DE TABLAS

Tabla 1: Personal encuestado. Fuente: Elaboración Propia……4

ABREVIATURAS, SIGLAS Y ACRÓNIMOS

A	
AWS	Sistema de Armas Autónomo
C	
CCAL	Centro de Control y Apoyo Logístico
COMINT	Inteligencia de Comunicaciones
E	
EA	Ataque Electrónico
ECM	Contramedidas Electromagnéticas
ED	Defensa Electrónica
EEM	Entorno Electromagnético
ELINT	Inteligencia Electrónica
EM	Espectro Electromagnético
EMO	Operaciones Electromagnéticas
EPM	Medidas de Protección Electromagnética
ES	Vigilancia Electrónica
ESM	Medidas de Apoyo de Guerra Electrónica
EW	Guerra Electrónica
EWCC	Células de Coordinación de EW
F	
FAS	Fuerzas Armadas
I	
IA	Inteligencia Artificial
R	
ROE	Reglas de Enfrentamiento
ROFAS	Reales Ordenanzas de las FAS
S	
SIGINT	Inteligencia de Señales
SOFA	Acuerdo sobre el Estatuto de las Fuerzas

1. INTRODUCCIÓN

En la actualidad, de entre todos los dominios en los que se desarrollan las operaciones militares, algunos, los más clásicos, como son el aire, la tierra y el mar han ido cediendo interés a favor de otros emergentes como el espacio, el ciberespacio o el electromagnético. Este último dominio no llegó a cobrar una importancia destacable hasta la Segunda Guerra Mundial, con la Batalla de Inglaterra en 1940 como punto de inflexión para su desarrollo acelerado en las siguientes décadas.

Desde entonces y lo que la tendencia parece marcar, la Guerra Electrónica[1] (en adelante, EW) y sus unidades se han convertido en piezas fundamentales para las fuerzas armadas, librando una batalla constante en un dominio silencioso en el que el desarrollo de la tecnología es cada vez más masivo, cambiante y disperso, y donde la clave del éxito es la velocidad de adaptación de cada ejército.

Hoy en día, los países desarrollados poseen una gran dependencia del Entorno Electromagnético (en adelante, EEM) tanto en el ámbito militar, como el ámbito privado y comercial con el desarrollo de tecnologías de la información, streaming[2], etc. Esto genera una fuente inagotable de oportunidades para lograr la ventaja y superioridad sobre el adversario, a la vez, presenta una gran cantidad de potenciales vulnerabilidades. De esta manera, se pueden realizar Operaciones Electromagnéticas (en adelante, EMO) de diversa naturaleza, desde maniobras psicológicas que busquen mermar la moral del adversario, hasta acciones directas que traten de influir en su toma de decisiones.

Según la publicación doctrinal de EW (Mando de Adiestramiento y Doctrina, 2009), la EW divide sus EMO en tres acciones diferentes atendiendo a sus efectos, Ataque Electrónico (en adelante, EA), Defensa Electrónica (en adelante, ED) y Vigilancia Electrónica (en adelante, ES). Para lograr tales efectos, las unidades de EW centran sus actividades mediante la integración de acciones por medio de Medidas de Apoyo de Guerra Electrónica, (en adelante, ESM), Medidas de Protección Electromagnética (en adelante, EPM) y Contramedidas Electromagnéticas (en adelante, ECM), siendo estas últimas, de carácter defensivo y sobre las que se centrará el trabajo.

Son numerosos los ejemplos en los que la EW terminó por inclinar la balanza hacia un contrincante u otro, ejemplo de ello es la mencionada Batalla de Inglaterra, en la que los alemanes perdieron por la eficacia de los radares británicos. Un ejemplo más reciente es lo que estamos viendo en el conflicto de Ucrania, según el oficial de EW de EE.UU. Jeffrey H. Fischer en el periódico de The Defense Post, (2022), la minimización de la importancia de la Inteligencia de Comunicaciones (COMINT), Inteligencia Electrónica (ELINT) e Inteligencia de Señales (SIGINT, que consiste en una combinación de COMINT y ELINT) por parte de Rusia fue clave para que Ucrania pudiera resistir durante los primeros días de conflicto.

---

[1] *La publicación doctrinal de EW (Mando de Adiestramiento y doctrina, 2009) define la EW como la disciplina militar que consiste en explotar el espectro electromagnético en propio beneficio e impedir su uso al adversario. Sus acciones se materializan mediante operaciones electromagnéticas.*

[2] *Según Cambridge Dictionary (Cambridge University Press, 2022), streaming es la tecnología que permite ver y oír contenidos que se transmiten desde internet u otra red sin tener que descargar previamente los datos al dispositivo desde el que se visualiza y oye el archivo.*

Este auge de las EMO ha puesto de manifiesto la existencia de una jurisprudencia insuficiente y desactualizada acerca de su empleo en la mayoría de los países democráticos, provocando problemas de seguridad, como la reticente utilización de medios de EW en diferentes zonas de operaciones, por la gran potencia y repercusión legal que tiene el empleo de estos. El problema se fundamenta en que los sistemas de EW y las EMO pueden comprometer las libertades y derechos de los ciudadanos, en cuyo caso, parece no haber una jurisprudencia clara en cuanto al tratamiento de responsabilidades.

Además, el auge paralelo en el desarrollo de Sistemas Autónomos de Armas (en adelante, AWS), que implementan Inteligencia Artificial (en adelante, IA), amplia considerablemente las lagunas existentes en cuanto a la responsabilidad del mando[3].

Por otro lado, la IA involucra un aprendizaje autónomo por medio de complejos algoritmos que se actualizan por si solos, sin necesidad de intervención humana, dicho de otra forma, los algoritmos de la IA se programan ellos mismos a partir de unas instrucciones básicas que define el programador. Este hecho, es fundamental para entender la complejidad a la hora de regular la responsabilidad del mando con estos sistemas, si bien es cierto que se pueden establecer límites de comportamientos independientemente de lo que la IA pueda "aprender", la realidad es que no hay consenso en cómo abordar esta situación.

Este Trabajo Fin de Grado continua la investigación iniciada por el comandante Eduardo Lobo Almazán en su Trabajo Final de Máster "Uso de la Fuerza y Responsabilidad del Superior" (2022) y pretende abordar la problemática anterior, estableciendo las bases jurídicas para que regulaciones futuras puedan dar una respuesta satisfactoria y eficiente en un dominio etéreo, pero con una creciente importancia como es el electromagnético.

En palabras del coronel Pedro Baños Bajo, en el XXVIII Curso Internacional de Defensa, Seguridad y Defensa: Una mirada al futuro, celebrado en Jaca (Huesca) (2021), *"la guerra actual y la guerra del futuro se lleva a cabo mediante acciones de información, desinformación, negación de servicios, campañas psicológicas, etc"*, Con esto, el coronel se refiere a las acciones en las que las unidades de EW tienen capacidades para operar. La realización de este trabajo se sustenta en esta realidad, en la que los países llevan a cabo EMO a diario mientras se carece de una jurisprudencia que las pueda regular.

Este trabajo se ha desarrollado con el apoyo de la Compañía de Guerra Electrónica Ligera 1/II/31 cuya composición orgánica se adjunta en el Anexo I.

[3] Entendiendo la IA como una tecnología desarrollada para ejecutar trabajos de forma autónoma y sin depender de ningún operador humano. Y considerando los AWS como sistemas de armas que son capaces, una vez activados, de seleccionar, discriminar y atacar objetivos sin ningún tipo de intervención humana. Este concepto de AWS, no elimina la supervisión de un operador que puede estar presente o no durante el desempeño de la actividad de su actividad. En esta línea, resulta evidente que los AWS ponen de manifiesto cuestiones legales y éticas en la relación operador-arma.

2. OBJETIVOS Y METODOLOGÍA

2.1. Objetivo y alcance

El objetivo general de este trabajo fin de grado es definir unos cimientos sólidos sobre los que se pudiera apoyar una jurisprudencia futura relativa a la responsabilidad del mando en el empleo de ECM.

Para ello, y de forma secuencial, se plantean los siguientes objetivos específicos:

- Conocer las capacidades de los medios de EW y AWS de las que dispone España en zona de operaciones.
- Definir las capacidades futuras que podrían proporcionar el desarrollo de medios nuevos de EW con la aplicación de IA.
- Analizar la jurisprudencia nacional e internacional existente respecto a la responsabilidad del mando en el empleo de ECM.
- Plantear el tratamiento de responsabilidad en diversos casos de estudio que pudieran darse en el futuro y pongan de manifiesto la necesidad de la creación de una regulación específica sobre AWS y su determinación de responsabilidades.
- Analizar la problemática en la determinación de responsabilidades en sistemas con IA.
- Establecer las tendencias y líneas de acción en las que se pudieran apoyar regulaciones próximas.

El alcance de este Trabajo Fin de Grado se focaliza en el empleo de ECM. Por un lado, el trabajo trata de definir las capacidades de EW en zona de operaciones de las que dispone España, no solo las actuales, sino también las líneas de acción en las que se están desarrollando nuevas tecnologías y capacidades futuras con la aplicación de IA.

Se analizará por otro lado, la jurisprudencia relativa a la responsabilidad del mando en la aplicación de ECM, tanto en el ámbito nacional, como en el ámbito internacional. Para ello, se plantearán posibles casos de estudio y supuestos que pudieran ocurrir con el desarrollo y empleo de nuevas tecnologías, en los que la responsabilidad de dichas acciones parece estar menos definida cada vez. Además, se realizarán elucubraciones relativas a posibles regulaciones futuras que pudieran resolver las incompatibilidades, vacíos o problemáticas surgidas a raíz del desarrollo de la IA y otras tecnologías, ya que la velocidad de su desarrollo deja atrás legislación aplicable.

Finalmente, se expondrán las conclusiones, basadas en el análisis documental y entrevistas realizadas a militares con gran experiencia en unidades de EW en España. Del mismo modo, se ofrecerá una opinión personal sobre la perspectiva futura en este ámbito de defensa.

2.2. Metodología

Para la realización del trabajo se seguirán una **metodología cualitativa** manteniendo una perspectiva general y objetiva.

2.2.1. Revisión documental

La metodología seguida se inicia con la revisión documental, tanto a nivel nacional como internacional de la normativa relativa a la regulación de la responsabilidad del mando y su tratamiento jurisprudencial. Esta revisión documental será fundamental para determinar las carencias de la jurisprudencia actual y las posibles problemáticas futuras.

Del mismo modo, se ha accedido al portal del conocimiento de la intranet del Ejército de Tierra, obteniendo publicaciones relativas a la EW y sus operaciones. Además, se ha accedido a la página de Sharepoint de la Cía EWL 1/II/31 recopilando manuales de uso de sus equipos, lo que ha permitido la determinación de sus capacidades teóricas.

2.2.2. Entrevistas

Posteriormente al proceso de revisión documental, se ha realizado tres entrevistas individuales con preguntas abiertas a integrantes del Regimiento de Guerra Electrónica 31 (ver Tabla 1), todos ellos expertos en EW y con gran experiencia en su aplicación.

Las preguntas de la entrevista se adjuntan en el Anexo III. Se trata de nueve cuestiones que han tenido la finalidad de averiguar las capacidades reales de los medios de EW españoles y de recoger opiniones personales sobre tendencias y capacidades próximas. Además, han permitido mostrar los problemas que experimentan a diario o que podrían tener en futuros despliegues los propios medios de EW. Para ello, y por la naturaleza de la información tratada, se firmó un Acuerdo de Confidencialidad (Ver Anexo II) con cada entrevistado. Este acuerdo de confidencialidad se adaptó a las necesidades de la situación partiendo de un modelo acuerdo de confidencialidad publicado por el Portal Jurídico A Definitivas (A Definitivas, 2022).

El personal entrevistado fue seleccionado y contactado personalmente (ver Tabla 1). Cada entrevista resulta de especial interés, ya sea por el puesto que el entrevistado ocupa en el desarrollo e investigación de nuevos medios o bien, por su experiencia en despliegues de diferentes naturalezas en zona de operaciones.

Empleo y Nombre	Puesto	Destino
Teniente Jorge Robles Carpio	Oficial Cía. EWL	REW 31
Brigada Ricardo Rodríguez Baña	Miembro CCAL	REW 31
Sargento Yone Armas Pérez	Suboficial Cía. EWL	REW 31

Tabla 1: Personal encuestado. Fuente: Elaboración Propia

2.2.3. Estudio de casos

A partir de la información recopilada en la revisión documental y en las entrevistas, se plantean una serie de casos reales y supuestos que pretenden evidenciar la carencia de una jurisprudencia eficiente y clara a la vez que la dificultad para establecer responsabilidades conforme avanza el desarrollo tecnológico.

Siguiendo los ejemplos de cada caso y las tendencias en el desarrollo de nuevos medios, se procederá a elucubrar las bases para que regulaciones futuras no queden desactualizadas tan rápidamente y puedan proporcionar un marco legislativo duradero.

3. ANÁLISIS DEL MARCO JURÍDICO ACTUAL

A continuación, se muestra el marco jurídico nacional e internacional relativo a la responsabilidad del mando. Ambos marcos jurídicos constituyen la casilla de salida para la realización de este Trabajo Final de Grado y son el resultado de la revisión documental realizada.

3.1. Marco Legal Español

España tiene el honor de ser uno de los países pioneros en tratar de regular la responsabilidad del mando durante los siglos XVIII y XIX. Ejemplo de ello son el artículo 155 del Código Penal de la Marina de Guerra de 1888 o el artículo 391 del Código de Justicia Militar de 1945.

Todas las regulaciones que se desarrollaron tienen en común el reconocimiento de la responsabilidad indirecta del mando, por ser el responsable de que sus subordinados actuaran de acuerdo a las leyes y usos de la guerra y sin cometer delitos en el empeño de sus funciones.

En España, el ordenamiento jurídico que regula la responsabilidad del mando lo hace mediante la Ley Orgánica 14/2015 del Código Penal Militar (Gobierno de España, 2003) y el Código Penal (Gobierno de España, 1995).

Por otro lado, se tendrá en consideración en lo relativo a la responsabilidad del mando las Reales Ordenanzas de las Fuerzas Armadas[4] (ROFAS) (Ministerio de Defensa, 2009) y en la Ley Orgánica de Derechos y Deberes de los miembros de las Fuerzas Armadas (Gobierno de España, 2011).

3.1.1. Ley Orgánica 14/2015 del Código Penal Militar

En primer lugar, para comprender el concepto de mando se debe recurrir al artículo 5 de la Ley Orgánica 14/2015, de 14 de octubre, del Código Penal Militar (Gobierno de España, 2015), que define: “Es superior el militar que, respecto a otro, ostente empleo jerárquicamente más elevado, o ejerza autoridad, mando o jurisdicción en virtud del cargo o función que desempeñe como titular o por sucesión reglamentaria”.

La misma publicación en su artículo 64 determina la responsabilidad del mando:

> El militar con mando de fuerza o unidad, Comandante de buque de guerra o aeronave militar que no mantuviera la debida disciplina en las fuerzas a su mando, tolere a sus subordinados cualquier abuso de autoridad o extralimitaciones de sus facultades o no procediere con la diligencia necesaria para impedir un delito militar será castigado con la pena de tres meses y un día a cuatro años de prisión, pudiendo imponerse, además, la pena de pérdida de empleo o, en su caso, la inhabilitación absoluta para el mando de buque de guerra o aeronave militar.

[4] *Normas que determinan los derechos y deberes del militar comprendidos por valores morales y principios éticos.*

Es importante destacar que el artículo 64 solo responsabiliza al mando en delitos cometidos por sus subordinados en caso de que estos sean tolerados o inobservados por el mismo. Es decir, al mando se le responsabiliza por omisión, atendiéndose a las acciones no tomadas para preservar el Derecho Internacional Humanitario[5] (en adelante, DIH) y la falta de supervisión o de control de sus subordinados. Sin embargo, no se le responsabilizada explícitamente por estos mismos. De manera que esta regulación parece insuficiente al no regular la responsabilidad directa del mando en las situaciones que se pueden dar en la actualidad.

Apareciendo así el concepto de responsabilidad por omisión, en la que debe existir una relación mando-subordinado. Basándose así, en el supuesto de la inacción del mando para establecer las medidas que considere oportunas a su alcance para evitar los delitos de los que tuviese conocimiento.

En la misma línea, en los artículos 55 y 56 de las ROFAS (Ministerio de Defensa, 2009), se determina que la responsabilidad del mando militar no es renunciable ni compartida y que el mando será consciente de las responsabilidades penales graves en delitos contra el DIH. Si bien es cierto que las ROFAS carecen por completo de carácter jurídico y únicamente constituyen una guía moral y ética para el militar, se le atribuye al mando una responsabilidad moral y ética con su país.

3.1.2. Código Penal

El artículo 615 bis de la Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Gobierno de España, 2003), determina la responsabilidad de la autoridad o del jefe militar. Este artículo hace referencia a los delitos comprendidos en los capítulos II, II bis y III del mismo título (delitos de genocidio, lesa humanidad y contra las personas y los bienes protegidos en caso de conflicto armado respectivamente).

Por otro lado, en el artículo 134 de la Ley Orgánica 2/1989, de 13 de abril, Procesal Militar (Gobierno de España, 1989) establece que:

> El militar que presenciare o tuviere noticia de la perpetración de cualquier delito de la competencia de la jurisdicción militar, está obligado a ponerlo en conocimiento, en el plazo más breve posible, del Juez Togado Militar, o del Fiscal Jurídico Militar, o de la Autoridad Militar que tuviere más inmediatos.

El resultado de estos dos artículos es que el Código Penal hace una clara distinción entre el mando militar que no evita la comisión de un delito y para el que establece las mismas penas que para el subordinado que lo comete. Que el mando militar que presenciando o teniendo conocimiento no informase a la autoridad correspondiéndote, para el que sería tratado de forma diferente respecto del subordinado que lo comete.

[5] *Disciplina del Derecho Internacional Público que regula las normas y usos de los conflictos armadas para proteger, por razones humanitarias, a las personas que no participan en las hostilidades.*

3.1.3. Obediencia del subordinado

En las Fuerzas Armadas (en adelante, FAS), por su propia estructura jerarquizada, aparece el concepto de obediencia debida del subordinado. El subordinado podría no ser responsable de los hechos que pudieran constituir delitos derivados de sus acciones, ya que actuaría cumpliendo órdenes de su mando y conforme a su deber.

Los artículos 410 y 411 del Código Penal (Gobierno de España, 1995) regula y define las características de un delito de desobediencia. Por su parte, el subordinado podría alegar cumplimiento del deber, miedo insuperable, estado de necesidad o desconocimiento de la ilegalidad de la orden para evitar así su responsabilidad.

Por otro lado, el artículo 44 y 45 del Código Penal Militar (Gobierno de España, 2003) no consideran la obediencia debida en ningún momento, definiendo la disciplina como medio para asegurar el riguroso cumplimiento del deber y determinando que todo militar obedecerá las órdenes.

Sin embargo, en el artículo 48 de las ROFAS (Ministerio de Defensa, 2009) se establecen los límites de la obediencia. Se expone así que el militar no estará obligado al cumplimiento de las órdenes que puedan constituir delitos, pero en tal caso, asumirá la responsabilidad de su incumplimiento.

A la vista de la jurisprudencia expuesta sobre la obediencia debida del subordinado, no hay coherencia entre el Código Penal Militar y el Código Penal. Si el mando o el militar que ejerza mando cometiese un acto constitutivo de delito sería juzgado, por su condición de militar conforme al Código Penal Militar, y por su condición de ciudadano conforme al Código Penal, asumiendo las responsabilidades correspondientes. En este sentido, en el ámbito interno de las FAS no podría alegar obediencia debida, pero en el ámbito general del Código Penal sí.

3.2. Marco Legal Internacional

El marco legal internacional sobre la responsabilidad del mando viene definido en el Derecho Internacional Público, el cual establece el principio de responsabilidad penal del superior jerárquico y no solo del mando militar. Por lo que, a partir de este momento y en este apartado se hablará de superior, pudiendo ser un mando militar o un superior jerárquico en el ámbito civil.

De esta manera, el Derecho Internacional Público trata la responsabilidad penal del superior en las disciplinas de DIH, Derecho Penal Internacional y en el Derecho Internacional de Derechos Humanos. Centrándose la regulación internacional que a continuación se expone en el DIH, por ser el que limita y restringe los medios y actuaciones para hacer la guerra, protegiendo tanto a combatientes como a personas que no participan en las hostilidades o que hayan decidido dejar de hacerlo además de los posibles bienes que se puedan ver afectados.

Fundamentalmente, la jurisprudencia internacional actual se desarrolló a consecuencia de la celebración del Tribunal Militar Internacional de Extremo Oriente[6] y del Tribunal Internacional de Nuremberg[7] en los que fueron juzgados militares de alto cargo y en los que se sentaron las

[6] *Tribunal que celebró los Juicios de Tokio, en los que se juzgaban los posibles crímenes de guerra que pudo cometer Japón tras la Segunda Guerra Mundial.*

[7] *Tribunales celebrados por el bloque vencedor (Naciones Aliadas) tras la Segunda Guerra Mundial. En ellos se juzgaron a los principales superiores jerárquicos por los posibles crímenes de guerra que pudieron*

bases por primera vez para definir la responsabilidad del superior en relación a crímenes cometidos por sus subordinados.

Posteriormente, estas bases serían perfeccionadas en el Convenio de Ginebra de 1949, el Protocolo Adicional I de 1977, el Derecho Consuetudinario, los Tribunales Penales Internacionales ad hoc y el Estatuto de Roma de 1998 de la Corte Penal Internacional.

3.2.1. Protocolo Adicional I de 1977

El Protocolo Adicional I, en el artículo 86 (2) (Comité Internacional de la Cruz Roja, 1977) referente a omisiones establece que:

> El hecho de que la infracción de los convenios o del presente Protocolo haya sido cometida por un subordinado no exime de responsabilidad penal o disciplinaria, según el caso, a sus superiores, si estos sabían o poseían información que les permitiera concluir, en las circunstancias del momento que ese subordinado estaba cometiendo o va a cometer tal infracción si no tomaron todas las medidas factibles que estuvieran a su alcance para impedir o reprimir esa infracción.

Complementando al artículo anterior, el artículo 87 (3) del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977) relativo a los deberes del jefe establece que:

> Las Altas Partes contratante y las Partes en conflicto obligarán a todo jefe que tenga conocimiento de que sus subordinados u otra persona bajo su autoridad van a cometer o han cometido una infracción de los Convenios o del presente Protocolo a que se tome las medidas necesarias para impedir tales violaciones de los Convenios o del presente Protocolo y, en su caso necesario, promueva una acción disciplinaria o penal contra los autores de violaciones.

Se aprecia entonces que, el superior solo asume responsabilidades por omisión en el caso de que tenga conocimiento. El Protocolo Adicional I no determina ninguna otra responsabilidad por parte del superior a la ya mencionada en la regulación nacional, de manera que, la regulación nacional sigue la misma línea que la regulación internacional. Sin embargo, este conocimiento debe ser demostrado y no supuesto únicamente por su condición de superior, algo que puede ser difícilmente realizable en el caso de conflictos armados como es una guerra.

cometer en nombre del Tercer Reich.

3.2.2. Derecho Consuetudinario

La norma 153 del Derecho Internacional Humanitario Consuetudinario (Henckaerts and Doswald-Beck, 2007) establece que:

> Los jefes y otros mandos superiores son penalmente responsables de los crímenes de guerra cometidos por sus subordinados si sabían, o deberían haber sabido, que estos iban a cometer o estaban cometiendo tales crímenes y no tomaron todas las medidas razonables y necesarias a su alcance para evitar que se cometieran o, si ya se habían cometido, para castigar a los responsables.

De nuevo, el Derecho Consuetudinario continúa determinando una responsabilidad por omisión a los superiores de los crímenes cometidos por sus subordinados. Sin embargo, el ámbito de aplicación del Derecho Consuetudinario es más amplio, aplicándose en las naciones tanto para conflictos armados internacionales como conflictos armados internos.

3.2.3. Estatuto de Roma de 1998 de la Corte Penal Internacional

En el Estatuto de Roma de 1998 (Corte Penal Internacional, 1998), relativo a la responsabilidad de los jefes y otros superiores se encuentra el artículo 28. Este artículo no aporta nada nuevo ya que continua con lo expresado la norma 153 del Derecho Consuetudinario y sigue la misma línea que lo anterior.

El artículo 28 concierne tanto a civiles como a militares y es aplicable tanto a fuerzas armadas estatales como grupos armados privados, así como superiores que ostenten un control sobre sus subordinados. Siguiendo la idea de la jurisprudencia expuesta anteriormente, se aplica sobre conductas que el responsable debería de haber sabido y no sobre lo que conocía en el momento.

3.2.4. Conflicto Armado Nacional

En lo que respecta a los conflictos armadas no internacionales, la realidad es que cada vez más naciones desarrollan regulaciones penales acerca de la responsabilidad del superior respecto a los posibles crímenes de guerra que se pudieran cometer. No es el caso de España, que continúa aplicando la regulación propia del Código Penal y del Código Penal Militar.

Además, como se ha dicho anteriormente, la norma 153 del Derecho Consuetudinario (Henckaerts and Doswald-Beck, 2007) es aplicable también en conflictos armados internos, por lo que, en el caso de España, la responsabilidad que se podría atribuir al mando en el caso de un conflicto armada interno sería únicamente una responsabilidad por omisión.

4. DETERMINACIÓN DE CAPACIDADES DE EW

La Cía. EWL 1/II/31 es la única unidad del Ejército de Tierra que cuenta con medios de EW tácticos y desplegables en zona de operaciones. A continuación, se exponen las principales capacidades de EW y ECM con las que cuenta esta compañía y, en consecuencia, España.

4.1. Medios EW

Las ECM son todas aquellas medidas referentes a acciones con la finalidad de reducir o impedir el uso hostil del espectro EM por parte del enemigo, empleando la propia energía electromagnética.

Según la publicación doctrinal de EW (Mando de Adiestramiento y Doctrina, 2009), las ECM se dividen en tres tipos de acciones (ver Ilustración 1):

- **Perturbación Electrónica:** Es la emisión deliberada o reflexión de energía electromagnética con la finalidad de comprometer la eficacia de los medios y sistemas del enemigo.
- **Decepción Electrónica:** Es la emisión deliberada, alteración, absorción o reflexión de energía electromagnética con el fin de confundir o engañar al enemigo y a sus propios sistemas.
- **Neutralización Electrónica:** Consiste en el empleo intencionado de la energía electromagnética para perjudicar, ya sea de forma permanente o temporal, los equipos enemigos que basan su funcionamiento únicamente en el EM.

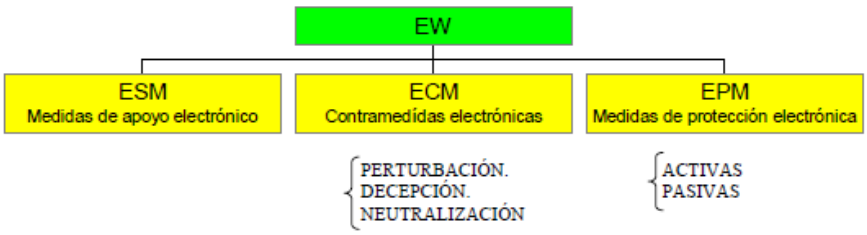

Figura 1: Medidas de EW. Fuente: ACART-VA-005

Sin embargo, la Cía. EWL 1/II/31 no solo centra sus capacidades en ECM, sino que, como queda reflejado en las respuestas de las diferentes entrevistas, España posee capacidades de EW en todo el espectro de medidas.

Conforme a la pregunta 3 del Anexo III, las capacidades actuales de la Cía. EWL 1/II/3, quedan divididas en tres medios diferentes (No se nombrará ni tratarán los equipos específicos por motivos de confidencialidad):

- **Radiofrecuencia:** España consta de varios equipos con capacidades de interceptación y goniometría en todo el espectro que ocupa las bandas de radio analógica y SDR[8].
- **Telefonía móvil:** Con capacidades de interceptar comunicaciones hasta tecnologías 4G y de obtener el posicionamiento global del terminal. Además de la posibilidad de realizar escuchas pasivas en redes con tecnología 2G.
- **Telefonía Satélite:** Los medios se centran en las tres principales compañías privadas que ofrecen servicio de comunicación vía Satélite (IRIDIUM, INMARSAT y THURAYA). Las capacidades en telefonía satélite se centran en la interceptación y obtención de la información del satélite.

Tanto el teniente Robles como el sargento Armas explicaron (ver pregunta 4 del Anexo III) que, la Cía. EWL 1/II/31 tiene dos formas de trabajar diferenciadas: Por un lado, la compañía tiene la misión de obtener información con medios satélites, radiofrecuencia y telefonía móvil con la que posteriormente se pueda generar inteligencia sobre posibles células enemigas o dispositivos móviles de los que no se tuvieran conocimiento. Por otro lado, la compañía puede actuar como Force Protection[9], integrándose dentro del propio despliegue de la unidad a la que apoya y operando por oportunidad, es decir, interceptando comunicaciones que puedan despertar una alerta temprana[10] en la misión. Es por esta razón, que las principales capacidades de cada medio se centran en la interceptación, goniometría y obtención de información.

4.2. Medios AWS

En la actualidad, España no posee ningún tipo de AWS, sin embargo, dos de los entrevistados son mandos militares que desempeñan sus funciones dentro de un GAMO[11], de manera que conocen perfectamente los problemas y las demandas que requieren para su perfeccionamiento y las capacidades que actualmente se están demandando en cada despliegue.

Ambos mandos concuerdan que los medios AWS serán el futuro, ya que permitirán recortar en gran medida el tiempo de obtención de información para la generación de inteligencia. En esta línea, tanto el teniente Robles, como el sargento Armas señalaron (ver pregunta 6 del Anexo III) que, esperan que los nuevos AWS con implementación de IA podrían detectar señales, compararlas, demodularlas y clasificarlas, lo que permitiría realizar escuchas en tiempo real. Otra demanda de estos sistemas es que los AWS puedan traducir las escuchas de los idiomas o dialectos de interés al castellano o ingles directamente, además de clasificar su contenido en base a su relevancia. Este último sistema permitiría reemplazar la figura del interprete dentro de la tripulación de un GAMO,

[8] *Radio definida por software y que puede operar con diferentes tipos de modulaciones y frecuencias.*

[9] *Unidad encargada de proteger al personal militar, civil, equipos e instalaciones de las operaciones para mantener la eficacia operativa y contribuyendo al éxito de la misión.*

[10] *Alerta anterior a la posible amenaza que genera un estado en el que se refuerza la vigilancia y atención para evitar el riesgo que la generó.*

[11] *Estación de EW, generalmente montada sobre un vehículo, que cuenta con las capacidades de goniometría y adquisición en movimiento.*

pudiendo ser sustituida por otro operador, y resolviendo el gran problema de las traducciones y la fidelidad de estas.

Asimismo, los tres entrevistados están de acuerdo en que los nuevos AWS podrían generar nuevos impedimentos legales relacionados con la protección de datos y la privacidad de las comunicaciones. Algunos de ellos se tratarán posteriormente en los supuestos casos de estudio.

Respecto a las tendencias en el desarrollo de medios futuros, todo el personal entrevistado respondió en las preguntas 5 y 6 del Anexo III, que la línea de acción en la que se está trabajando actualmente es el desarrollo de AWS con implementación de IA con los que se pueda dotar al ejército de nuevas y mejores capacidades. Esto muestra que la implementación de la IA es una tendencia en la mayoría de los países y que será una realidad en poco tiempo a la vez que abre un amplio y diverso abanico de interrogantes, siendo uno de ellos, el tratamiento de responsabilidad del mando con estos sistemas.

Ante la tendencia en el desarrollo de nuevos medios con IA, es necesario aclarar, que la IA no es un arma por sí sola, sino un componente de un sistema de armas cuyo propósito es acelerar el proceso de toma de decisiones para obtener una ventaja militar.

Además, los tres entrevistados manifestaron que la IA, a pesar de ser el futuro, no parece ser la solución a todas las situaciones bélicas, ya que podrían darse casos de toma de decisiones erróneas por no contar con suficiente información o que requieran decisiones éticas para las que los algoritmos de IA no están preparados y que implicarían una responsabilidad individual del mando. Este supuesto también será tratado más adelante.

Principios éticos y técnicos en el empleo de IA

De acuerdo con lo anterior, el gobierno de EE.UU. publicó “Los cinco principios éticos que deben regir el uso de sistemas con IA en el ámbito de defensa” (Defense Innovation Board, 2020). Con esta publicación, el país puntero en el desarrollo de AWS, pretende definir unos principios básicos en la creación de nuevos sistemas de armas y guiar al resto de naciones a falta de una regulación específica al respecto. Los principios éticos y técnicos que deben seguir los sistemas que implementen IA son los siguientes:

- Sistemas Responsables: Los seres humanos tienen la obligación de aplicar un nivel de juicio apropiado, además, deben seguir siendo responsables durante el desarrollo y uso de los sistemas con IA.
- Sistemas Equitativos: Se deben tomar las medidas necesarias para evitar posibles sesgos no deseados que pudieran causar perjuicio a las personas.
- Sistemas Rastreables: El personal debe comprender la tecnología y sus aplicaciones operativas, la IA debe ser transparente y auditable.
- Sistemas Confiables: Las capacidades de IA deben ser seguras y efectivas y deben ser sometidos a pruebas a lo largo de su vida útil.
- Sistemas Gobernables: La IA debe estar diseñada de manera que permita su control y evitar consecuencias no deseadas.

Si bien es cierto que estos principios se enumeran como propuesta para el empleo de medios con IA y que estos no se encuentran recogidos en ninguna regulación internacional. Es razonable pensar que estos cinco principios podrían servir de guía para la creación de una futura jurisprudencia y resolver muchas de las actuales brechas existentes.

Capacidades futuras con la implementación de IA

El Brigada Baña, que cuenta con 17 años de experiencia en unidades de EW, y actualmente destinado en el Centro de Control y Apoyo Logístico (CCAL)[12], respondió en la pregunta 4 en el Anexo III que los actuales teatros de operaciones están demandando medios con capacidad de interceptación de comunicaciones, especialmente telefonía móvil. A la vez se demandan medios con capacidad de interceptación de aeronaves RPAS[13] controladas por radio-frecuencia. En la pregunta 6 del Anexo III, el Brigada Baña añadió a la pregunta anterior que, actualmente se está trabajando en la implementación de IA que pudiera capacitar a los RPAS para el análisis de imágenes con el que se permitiría identificar diversos medios enemigos. En el ámbito de las comunicaciones, la IA permitiría reconocer idiomas, dialectos o palabras claves para identificar posibles amenazas.

En la pregunta 8 del Anexo III, los tres entrevistados concuerdan en que los posibles impedimentos legales que pudiera haber referentes a la implementación de IA serían de posibles interceptaciones y escuchas de comunicaciones no autorizadas, sin embargo, en zona de operaciones, todas las medidas de EW están autorizadas y se ejecutan conforme las Rules of Engagement[14] (en adelante, ROE). En la siguiente pregunta, pregunta 9 del Anexo III, el Brigada Baña señaló que el desarrollo de nuevos medios con IA posiblemente cambie el tratamiento de responsabilidades pero que, según él, estos medios siempre estarían bajo la supervisión de un operador. Este operador, además del mando, tomaría responsabilidad en los sistemas con IA.

El supuesto anterior, relativo a una interceptación y escucha de una comunicación no autorizada resulta de especial interés, ya que podría comprometer el artículo 18 de la Constitución Española (Cortes Generales, 1978), que señala el derecho a la intimidad personal, y también será planteado posteriormente.

[12] *Unidad encargada de materializar las necesidades operativas en adquisiciones de equipos.*

[13] *Vehículo aéreo no tripulado, también conocido como UAV o DRON.*

[14] *Reglas que determinan las situaciones, forma e intensidad en la que una fuerza armadas puede emplear sus capacidades.*

5. RESPONSABILIDAD DEL MANDO EN AWS

A continuación, se analiza la jurisprudencia relativa a los AWS en el ámbito del DIH y la responsabilidad que asumiría el mando en el empleo de estos. Como se mostrará a continuación, en la actualidad la única jurisprudencia aplicable a AWS sería la regulación general de cualquier sistema de armas.

5.1. AWS y en el marco del DIH

A día de hoy no existe una jurisprudencia específica sobre el empleo de los AWS. Sin embargo, sí que existe una regulación general sobre las armas, cuyos estándares serían aplicables a los AWS. Esta regulación general se presenta a continuación.

El artículo 35 (1) del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977) determina que: “En todo conflicto armado, el derecho de las Partes en conflicto a elegir los métodos o medios de hacer la guerra no es ilimitado”.

El Protocolo Adicional I, en su artículo 36 (Comité Internacional de la Cruz Roja, 1977) también establece que:

> Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante.

Por otro lado, tanto en la norma 11 del Derecho Consuetudinario (Henckaerts and Doswald-Beck, 2007), como en el artículo 51 del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977), quedan prohibidos los ataques indiscriminados, quedando definidos dichos ataques en la norma 12 del Derecho Consuetudinario (Henckaerts and Doswald-Beck, 2007). De esta manera, se consideran ataques indiscriminados aquellos que:

a) No estén dirigidos contra fines militares específicos.

b) Se empleen medios que no permitan dirigir los ataques contra fines militares específicos.

c) Se empleen medios cuyos efectos no puedan ser limitados como exige el DIH.

Es decir, son ataques indiscriminados todos aquellos que puedan alcanzar tanto a objetivos militares como bienes o personas civiles indistintamente

Se entiende entonces, que conforme se desarrollen nuevos medios AWS que integran IA, estos deberán ser sometidos a una revisión en la que se realizaran pruebas y evaluaciones en entornos operativos similares en los que serán usados para garantizar que cumple los requisitos del DIH. El objetivo de esta revisión es garantizar, como dice el artículo 35 (2) del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977), que no se produzcan males superfluos o sufrimientos desproporcionados e incensarios de acuerdo a la ventaja militar que se espera obtener.

Al mismo tiempo, para que un AWS sea considerado legal, este debe de poder ser controlable y dirigible hacia objetivos militares. No obstante, los artículos mencionados, no especifican qué pruebas son necesarias, dejando abierto este aspecto a criterios de cada país.

Ilustrativo de esto es el ejemplo de EEUU, que siendo uno de los países punteros en el desarrollo de nuevos sistemas de armas y sin formar parte del Protocolo Adicional I, lleva a cabo importantes pruebas para asegurarse de que todas sus innovaciones cumplen con los tratados y acuerdos internacionales.

De acuerdo con lo anterior y como es de esperar, en ocasiones la legalidad o no de un sistema de armas nuevo es discutible en función de qué estado interpreta dicha legalidad. Un ejemplo de esto fue la Guerra de Vietnam en la que EEUU comenzó a utilizar municiones de racimo[15] o napalm[16], armas que actualmente se encuentran prohibidas por no cumplir con el artículo 35 (2) del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977) al causar sufrimientos innecesarios.

Hoy en día, continúa sin haber consenso entre los estados acerca de los AWS, una razón posiblemente sea porque los estados que desarrollan y utilizan los nuevos sistemas de armas y quiénes deciden sobre ellos poseen intereses distintos.

De esta situación en la que aparecen discrepancias entre estados a la hora de determinar la legalidad de nuevos sistemas de armas, como los AWS, se sugiere el desarrollo de nuevas jurisprudencias que aclaren y armonicen las consideraciones de necesidad militar y humanidad como dice el artículo 1 (2) del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977).

Es importante aclarar que, la implementación de IA en AWS, no determinará si el propio AWS es legal o no ya que no existe ninguna regulación en la actualidad que prohíba el empleo de IA.

Por otro lado, complementario al artículo 51 del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977), es el artículo 58 de la misma regulación. Este artículo establece que los países enfrentados se esforzarán y tomarán las medidas necesarias para alejar de la población civil los posibles objetivos militares y así protegerlos de los posibles daños colaterales. En este sentido, y sin ser requisito legal, los AWS con IA deberían contar con medidas de seguridad, advertencia y control como:

- Posibilidad de anular las funciones a criterio del mando.
- Capacidad para ser controlada por humanos.
- Capacidad para confirmar el control por humanos.
- Restricciones geográficas.
- Restricciones temporales.
- Capacidad para permitir o no “aprendizaje autónomo”.
- Capacidad para volver a un estado anterior en caso de fallo crítico.

Atendiendo al sentido común, la medida de seguridad más eficiente podría ser la capacidad de ser controlados por humanos durante las operaciones y así poder anular las funciones. Sin embargo, este no es un requisito legal, y la mayoría de los AWS que implementan IA actúan de forma completamente autónoma durante las operaciones.

[15] *Bombas de fragmentación que liberan pequeñas bombas en el aire.*

[16] *Arma química compuesta por gasolina que se adhiere fácilmente a las superficies y genera una combustión prolongada.*

Este hecho plantea un desafío y abre la puerta a la creación de una jurisprudencia más restrictiva en la que el papel del ser humano este más presente, tanto en el desarrollo como en las operaciones. Esta regulación debería partir de la Cláusula Martens por la que se especifica que el DIH posee como fuentes del derecho los principios de humanidad y de conciencia pública.

5.2. Responsabilidad del mando en sistemas de armas con IA

La IA, al igual que todos los métodos y armas para hacer la guerra debe adaptarse al DIH, siendo el mando el responsable de que la IA cumpla dichos principios.

Al mismo tiempo e independiente del grado de participación del ser humano en los propios sistemas con IA o los AWS, resulta obvio que, las regulaciones de responsabilidad se vinculan a las personas y no a las maquinas.

Esto es fundamental para determinar la responsabilidad del mando, ya que la legalidad de los AWS con IA, y su tratamiento de responsabilidades dependerá del empleo que haga el mando de ellos y de las decisiones que tome. En esta línea se considera que la IA cambiará sustancialmente el proceso de toma de decisiones.

Un ejemplo de esto fueron los cohetes V-1 y V-2 que la Alemania nazi utilizó como armas para aterrorizar a la población (Alpert, 2021), por su incapacidad para poder ser dirigidos, impactando sobre áreas civiles. Del mismo modo, si los AWS con IA se programan o se utilizan para realizar ataques indiscriminados, el mando podría ser responsable, en las condiciones y según determina el artículo 64 de la Ley Orgánica 14/2015 del Código Penal Militar (Gobierno de España, 2003b) y la norma 153 del Derecho Consuetudinario (Henckaerts and Doswald-Beck, 2007).

Se entiende que, el mando debe comprender lo que los AWS pueden hacer en el entorno particular en el que se están utilizando, como cualquier otra arma. Deben saber cómo responde el sistema en el campo de batalla y cuáles son sus limitaciones. Sin embargo, no están obligados a comprender las complejidades de cómo funciona el sistema, la ciencia y la tecnología detrás de su desempeño. En el caso de que se demuestre que un AWS realiza ataques indiscriminados, el mando podría rendir cuentas al caer dentro de su ámbito de responsabilidad directa o individual.

No obstante, el hecho de que el mando sea responsable por “decisiones” propias de AWS sobre las que, posiblemente nunca tenga suficiente control, puede resultar injusto. Se abre entonces una laguna de responsabilidad que quedaría cubierta por el propio ejercicio del mando militar, en el que será responsable directa e individualmente y asumiendo que es parte de su deber. En esta línea, es tan “justo” responsabilizar al mando por errores cometidos en el empleo de AWS como responsabilizar al mando que ordenase un bombardeo sobre un objetivo militar y que terminase siendo un hospital.

Además de la responsabilidad descrita anteriormente, es evidente la responsabilidad moral y ética del mando al ordenar o autorizar operaciones, que sin bien pudieran no estar prohibidas, irían en contra de los principios éticos y morales del ser humano.

5.3. Tratamiento de responsabilidad en diversos estudios de caso

A continuación, se expondrán y analizarán diversos estudios de casos, interesantes porque hayan podido acaecer en la realidad o derivarse de acciones hipotéticas. Los tres casos han sido ambientados personalmente en circunstancias que resultan de especial interés y se analizarán atendiendo a la responsabilidad del mando relativa a la jurisprudencia expuesta en este trabajo y otras regulaciones específicas de para cada supuesto en particular.

5.3.1. Supuesto de escucha no autorizada

Supuesto práctico: Tras una escalada de fuerza e inestabilidad geopolítica, España ha decidido desplegar unidades en territorio nacional en previsión de un posible conflicto armado de carácter internacional. Una de sus unidades, la Compañía de EW 2/I/41 está destacada en Sevilla realizando ECM para interceptar y geolocalizar comunicaciones procedentes del posible enemigo. Los sistemas de EW, no distinguen las comunicaciones procedentes de ciudadanos españoles, de las que provienen del enemigo, de manera que, toda comunicación interceptada debe ser tratada y procesada con el fin de elaborar inteligencia.

Antes de analizar este supuesto práctico, es necesario explicar cómo trabajan los medios de interceptación de telefonía móvil, telefonía satélite y radio frecuencia. La mayoría de estos medios, interceptan cientos o miles de comunicaciones en un periodo de tiempo relativamente corto. De manera que, el operador puede elegir si guardar o no las comunicaciones captadas. La realidad es que, debido al volumen de datos que se llegan capturar, lo más común es guardar todos esos datos para que puedan ser tratados por el operador o analista de EW posteriormente.

Analizando el supuesto desde el punto de vista jurídico, el artículo 197.1 del Código Penal (Gobierno de España, 1995) determina que:

> El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Por otro lado, la Constitución Española (Cortes Generales, 1978) reconoce en el artículo 18.1 el derecho a la intimidad personal. Además, en el mismo artículo 18.3, se determina que: “Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.”

Según el artículo 197 del Código Penal (Gobierno de España, 1995), se entiende que una persona podría estar incurriendo en un delito grave de vulneración de la intimidad cuando no participa de forma activa en la conversación y se produzca la grabación de esta. Sin embargo, si esa persona si participa activamente en la comunicación, aún sin informar al resto de participantes de que se les está grabando y, por lo tanto, sin sus respectivos consentimientos, la grabación de la conversación si se consideraría legal. Además, este

artículo no solo se refiere a interceptaciones y grabaciones de comunicaciones como un posible delito de vulneración a la intimidad, sino también, como un posible delito de divulgación de secretos. En ningún caso se consideraría legal la difusión de una grabación, aun siendo esta legal o no.

En el caso de la EW, la interceptación de comunicaciones se realiza sin participar activamente en estas, por lo que, en este sentido, y sin autorización previa de un juez, motivada por una investigación en curso, el mando podría incurrir en un delito grave, según el citado artículo, ya sea por vulneración de la intimidad o divulgación de secretos.

Por otro lado, la situación tratada en este supuesto podría agravarse ante la posibilidad de violar uno de los derechos fundamentales recogidos en la Constitución Española en el artículo 18.1 (Cortes Generales, 1978), el derecho a la intimidad.

Ahora bien, el artículo 55 (1) de la Constitución Española (Cortes Generales, 1978) referente a la suspensión de los derechos y libertades determina que:

> Los derechos reconocidos en los artículos 17, 18, apartados 2 y 3, artículos 19, 20, apartados 1, a) y d), y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2, podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución. Se exceptúa de lo establecido anteriormente el apartado 3 del artículo 17 para el supuesto de declaración de estado de excepción.

El mismo artículo determina en el párrafo segundo que, una ley orgánica (Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio (Gobierno de España, 1981)), podrá regular la forma en la que los derechos fundamentales reconocidos en los artículos 17 y 18 de la Constitución Española podrían ser suspendidos. En tal caso, esa suspensión de derechos podrá ser de forma general o individual.

La Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio (Gobierno de España, 1981), en el artículo 32 (1), define el estado de sitio de la siguiente manera: “Cuando se produzca o amenace producirse una insurrección o acto de fuerza contra la soberanía o independencia de España, su integridad territorial o el ordenamiento constitucional, que no pueda resolverse por otros medios”

El supuesto descrito, se trata de una situación que amenaza producir un acto de fuerza contra la integridad territorial de España. En este sentido, la unidad desplegada de EW podría realizar interceptaciones y grabaciones de comunicaciones siempre y cuando el Gobierno de España, con autorización del Congreso de los Diputados, haya declarado el estado de sitio. Se entiende que, en tal supuesto, el mando será responsable si ordena hacer las interceptaciones no encontrándose en la situación anteriormente descrita, que justifique la necesidad, asumiendo así una responsabilidad directa. Si el mando no ordena, pero tiene conocimiento de que sus subordinados toman la decisión de hacer las citadas interceptaciones, sin intentar evitar dichas acciones, o tomar represalias contra los culpables, en este caso, el mando asumiría una responsabilidad por omisión.

Cabe mencionar que la situación anterior se centraría en una operación en territorio nacional. Sin embargo, en el caso del mismo supuesto, pero con unidades de EW desplegadas en el extranjero, la situación a valorar sería diferente. En tal caso, la responsabilidad del mando vendría definida por las ROEs de la operación en cuestión, esperándose que fueran más permisivas por motivos de seguridad. Esto ya ha ocurrido en otros despliegues españoles, como en Afganistán, en el que se entiende que cualquier conversación e interceptación puede ser un

potencial objetivo, en pro de la protección del personal, de las instalaciones, de los medios y equipos, etc.

Concluyendo este supuesto, el mando será responsable de los posibles crímenes cometidos por sus subordinados, siempre que, como marca el artículo 28 del Estatuto de Roma de 1998 (Corte Penal Internacional, 1998), dichos subordinados estén bajo su mando o autoridad y control efectivo, en los casos en que:

- Hubiera sabido o, en razón de las circunstancias del momento, hubiera debido saber que las fuerzas estaban cometiendo esos crímenes o se proponían cometerlos.
- No hubiere adoptado todas las medidas necesarias y razonables a su alcance, para prevenir o reprimir su comisión o para poner el asunto en conocimiento de las autoridades competentes, tratándose así de un posible caso de negligencia consciente o de "vista gorda".

El mando podría incurrir en un delito grave de violación de la intimidad o de revelación de secretos, si no actuara conforme al artículo anterior.

Como se puede apreciar, la responsabilidad del mando puede variar dependiendo de las condiciones de cada situación, encontrándose la legalidad o no de las ECM delimitada por una fina línea difusa que obliga al mando a ser especialmente precavido en su toma de decisiones.

5.3.2. Supuesto de error en un AWS con IA

Supuesto práctico: Un nuevo AWS es desplegado en el frente entre dos países en conflicto armado. El país que lo despliega argumenta que posee solamente capacidades defensivas y que, ha sido desplegado con carácter meramente disuasorio. El AWS que se despliega consta de una cámara, a través de la cual, un potente algoritmo de IA tiene la capacidad de seleccionar, evaluar e identificar vehículos enemigos que traten de cruzar la frontera. Además, el AWS puede realizar ataques selectivos si el operador lo ordena. Una noche, el AWS identifica un vehículo de transporte sanitario debidamente marcado, que transporta niños heridos, como si fuera un camión logístico del enemigo. El operador, sin comprobar la información, realiza un ataque en el que la ambulancia es destruida.

En este supuesto, se analizará la consecuencia principal de la destrucción de una ambulancia y por la que se produce el asesinato de niños en un conflicto armado.

El artículo 21 del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977) determina que: "Los vehículos sanitarios serán respetados y protegidos del modo previsto en los Convenios y el presente Protocolo para las unidades sanitarias móviles".

Por otro lado, y según el artículo 8 del Estatuto de Roma de 1998 (Corte Penal Internacional, 1998), se define como crimen de guerra: "Dirigir intencionalmente ataques contra edificios, material, unidades y medios de transporte sanitarios, y contra personal que utilice los emblemas distintivos de los Convenios de Ginebra de conformidad con el derecho internacional".

Además, en este supuesto se produce el fallecimiento de niños, que son figuras protegidas por el DIH en el caso de conflictos armados, como indica el artículo 77 del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977).

En lo relativo al mando con la responsabilidad que pudiera tener, y como se ha expuesto anteriormente en el artículo 28 del Estatuto de Roma de 1998 (Corte Penal Internacional, 1998), para que el mando pueda ser responsable por los crímenes cometidos por sus subordinados por medios de un AWS se deben dar las siguientes condiciones:

- El mando debería saber que sus subordinados podían cometer o cometieron dichos crímenes.
- Debe existir una relación explícita mando-subordinado.
- Que el mando en esas circunstancias no hubiese tomados las medidas que considerase necesarias para evitar tal crimen. En este sentido, debe existir causalidad entre la falta de medidas para prevenir el delito y su realización.

De esta manera, el mando debería ser consciente del delito que puede ser cometido por el subordinado al no contrastar la información del sistema y ejecutar el ataque con tan trágico desenlace. El mando debería saber que los operadores bajo estrés y realizando actividades repetitivas podrían incurrir en este tipo faltas y tomar las medidas necesarias y oportunas para su prevención.

Además, en este supuesto, el mando que ha desplegado el AWS debería conocer sus capacidades y limitaciones, como un posible fallo al actuar en condiciones de baja visibilidad, que pudieran dar lugar a acciones de ataques indiscriminados. Como especifica la norma 11 del Derecho Consuetudinario (Henckaerts and Doswald-Beck, 2007) y en el artículo 51 del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977), en esta situación, se trataría de un AWS que no cumpliera con los principios del DIH al realizar o permitir dicho ataque.

En esta línea y tendiendo a la jurisprudencia expuesta, el supuesto podría concluir con la responsabilidad del mando respecto al asesinato de niños, siendo figuras protegidas por el DIH, a consecuencia del crimen cometido por su subordinado. El mando sería responsable por esto y por el ataque y destrucción de vehículos de transporte sanitario.

5.3.3. Supuesto de perturbación en el espectro electromagnético

Supuesto Práctico: Ante una escalada de violencia en un país en el que se llevan a cabo una misión de estabilización, el jefe de una compañía de EW decide aumentar la potencia con la que sus estaciones realizan ECM, en concreto, perturbación de las comunicaciones. Con este propósito consigue perturbar todas las comunicaciones en la capital del país anfitrión. Sin embargo, y casi de inmediato, se produce un atentado terrorista en un hospital de la capital, lo que ocasiona una gran cantidad de heridos y fallecidos. Conforme pasa el tiempo, la situación empeora al no poder recibir ayuda los heridos de manera oportuna y al encontrarse perturbadas las comunicaciones de los diferentes medios de emergencia, bomberos, vehículos de transporte de heridos y aeronaves de evacuación medicalizada. Lo que provoca que el número de fallecidos aumente.

El análisis de la responsabilidad del mando en este supuesto es diferente, hasta ahora únicamente se ha expuesto la posible responsabilidad del mando por omisión o negligencia ya que es la única que queda definida en el DIH. Sin embargo, el mando también asume una responsabilidad individual por sus decisiones o acciones.

En esta línea, y al tratarse de una misión de estabilización que se lleva cabo en un tercer país, el empleo y potencia de las medidas de EW deberían quedar definidos en las ROEs de la

propia misión. Estas ROEs se conforman de acuerdo a tratados entre el país anfitrión y el país que realiza la misión y siguiendo los principios del DIH.

El artículo 10 del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977), sobre protección y asistencia determina que: “Todos los heridos, enfermos y náufrago, cualquiera que sea la Parte a la que pertenezcan, serán respetados y protegidos”.

Complementando al artículo anterior se encuentra el artículo 12 (1) del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977), sobre la protección de las unidades sanitarias y determina que: “Las unidades sanitarias serán respetadas y protegidas en todo momento y no serán objeto de ataque”.

Si bien es cierto que es un supuesto genérico y que no quedan definidas las ROEs específicas de la misión, estas deberían respetar los artículos anteriores en todos los aspectos y acciones previstas en la operación. Además, el respeto a los heridos se trata de un principio morales y éticos que impera en los ejércitos de países democráticos, en el caso de España, estos principios quedan recogidos en el artículo 106 de las ROFAS (Ministerio de Defensa, 2009).

Atendiendo a los artículos mencionados, el mando podría asumir una responsabilidad individual por no respetar las ROEs, considerando siempre que estas definieran una potencia de perturbación que garantizase las comunicaciones de los medios de emergencia.

Es importante aclarar que esa responsabilidad solo podría ser atribuida por incumplimiento de las ROEs y no por ninguna jurisprudencia existente ya que, como se ha expuesto, solo existe jurisprudencia que determina la responsabilidad del mando por omisión.

6. Propuesta para la creación de regulaciones futuras

Tras el proceso de proceso de revisión documental y del estudio de casos ha podido quedar patente la falta de una jurisprudencia tanto internacional como nacional que regule los AWS.

Esto es debido a que la creación y adaptación de las leyes existentes evoluciona considerablemente más despacio que la tecnología. La brecha existente es cada vez más amplia ya que cada vez los legisladores necesitan tener mayores y complejos conocimientos sobre la tecnología que tratan de regular en cuestión.

A continuación, se presenta una propuesta jurídica a nivel OTAN que pretende ser una posible solución al principal problema visto, existencia de una jurisprudencia ineficaz y desactualizada relativa a la responsabilidad del mando en el empleo de AWS. Con ella, se pretende constituir la base sólida sobre la que se creen regulaciones específicas.

Cabe mencionar, que la UE presentó en abril de 2021 el Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (European Commission, 2021). Esta propuesta sobre IA de la Unión Europea se ha utilizado como guía para la elaboración de la siguiente propuesta legislativa sobre los AWS en el ámbito OTAN. De aprobarse, convertiría a la UE en una organización pionera en tener una legislación específica sobre IA.

6.1. Objetivos de la propuesta

1. Los objetivos específicos de esta propuesta son los siguientes:

a) Proporcionar un marco normativo equilibrado y flexible que permita establecer unas condiciones mínimas para resolver los riesgos del desarrollo de AWS con IA.

b) Proporcionar un marco normativo coherente con otras políticas OTAN.

c) Asegurar que los AWS de los países miembros sean confiables, seguros y respetuosos con los valores presentes en el DIH.

d) Definir claramente la responsabilidad de cada persona que participa en el uso y empleo de AWS

6.2. Propuesta de regulación de AWS

Título I. Disposiciones Generales

Artículo 1: Ámbito de aplicación

1. La propuesta será aplicable a:

a) Empresas y desarrolladores de AWS independientemente de si se encuentran establecidos en un país OTAN o no.

b) Estados miembros de la organización que empleen AWS.

c) Cualquier sistema autónomo que implemente IA y que pueda ser utilizado como un arma.

2. No será aplicable a terceros estados u organizaciones internacionales que no formen parte de los tratados y convenios a nivel OTAN ya existentes.

Artículo 2: Definiciones

1) Sistema Autónomo de Armas (AWS): Sistema capaz de realizar tareas complejas sin intervención humana tales como identificar, seleccionar y atacar objetivos.
2) Inteligencia Artificial (IA): Software programado para realizar operaciones complejas y que serían propias del ser humano en un principio.
3) Mando: Persona física responsable de una operación y de la que dependen el resto de miembros (subordinados) de una unidad militar.
4) Operador: Persona física responsable de emplear un medio de acuerdo a un propósito.
5) Programador: Persona física o jurídica u organismo que programa un software de IA con fines lucrativos o de manera gratuita.
6) Proveedor: Persona física o jurídica u organismo que desarrolle un AWS con fines lucrativos o de manera gratuita.

Título II. Prácticas con AWS

Artículo 3: Prácticas prohibidas

1. En esta propuesta estarían prohibidas las siguientes prácticas con AWS:

a) El desarrollo de AWS cuya IA pueda modificar, mediante cualquier tipo de técnica, el comportamiento de una persona de manera que pueda influenciarla para que tome decisiones que amenacen su integridad física o psicológica.

b) Los AWS que aprovechando cierta vulnerabilidad física o mental de una determinada población puedan alterar su comportamiento, de manera que, estos puedan ser influenciados para tomar decisiones que amenacen su integridad física o psicológica.

c) Los AWS con capacidades de identificación biométrica[17] en entornos públicos salvo que por motivos de seguridad y por orden judicial sea necesario.

d) Los AWS con capacidad de realizar ataques indiscriminados.

e) Los AWS que no cumplan con las debidas herramientas de seguridad, control y advertencia para reducir todo lo posible las consecuencias de un posible fallo de la naturaleza que sea.

f) El empleo de AWS en fase de pruebas o sin una correcta evaluación y sin conocerse exactamente su comportamiento y limitaciones en un entorno real.

g) El empleo de AWS por parte de personal que no comprenda de forma precisa los mecanismos, capacidades y limitaciones del sistema.

[17] *Tecnología que permite la identificación de personas a través de sus rasgos únicos.*

h) El empleo de AWS que no cumplan cualquier regulación o tratado internacional de la que los estados miembros de OTAN son parte.

Título III. Sistemas de AWS

Artículo 4: Cumplimiento de condiciones

1. Los AWS deberán cumplir con los requisitos expuestos en este Título.

Artículo 5: Requisitos de AWS

1. Los AWS deberían cumplir con los siguientes requisitos.

a) Para que un AWS pueda ser verificados, se evaluará en base a su finalidad prevista, sus potenciales riesgos y deberá contar con un sistema de gestión de riesgo. Este sistema de gestión de riesgos deberá ser un proceso reiterativo durante toda la vida útil del sistema.

b) Los AWS deberán ser sometidos a pruebas en condiciones similares en las que serán utilizados con el fin de poder definir claramente sus limitaciones y capacidades reales.

c) En aquellos algoritmos de IA de AWS que impliquen un autoaprendizaje del sistema, se le deberá proporcionar una base de datos inicial sin errores y completa de manera que permitan su aprendizaje y evaluación.

d) La documentación técnica de un AWS se mantendrá debidamente actualizada.

e) Los AWS serán diseñados y desarrollados de manera que sea posible el registro y trazabilidad de su actividad de forma automática. Este registro debe permitir el análisis y control del sistema en el caso de que el AWS presente un fallo y que pueda dar a un potencial riesgo.

f) Los AWS deben de ser capaces de presentar la información de salida completa y suficientemente clara garantizando su correcta interpretación por parte del operador.

g) Los proveedores de AWS deben proporcionar a los estados un manual de usuario en el que se especifiquen claramente sus capacidades, limitaciones y finalidad. Además, el manual deberá incluir protocolos de actuación ante cualquier circunstancia previsible que pueda generar un fallo en su funcionamiento.

h) Los AWS deben permitir su vigilancia y supervisión constante por personas físicas durante toda su vida útil. El proveedor del AWS deberá definir las medidas necesarias de supervisión humana.

i) Los AWS deben de poder asegurar un nivel de ciberseguridad, eficacia y precisión durante toda su vida útil.

Artículo 6: Deberes de proveedores, usuarios y programadores de AWS.

2. Los proveedores de AWS:

a) Serán responsables de que los AWS cumplan con los requisitos del Artículo 5.

b) Deberán implementar un sistema de control de calidad.

c) Elaborarán la documentación técnica del AWS.

d) Deberán asegurarse de que el AWS cumple con las capacidades y limitaciones que figuran en su ficha técnica.

e) Deberán corregir y adoptar las medidas que considere necesarias para que el AWS que no cumpla con los requisitos del Artículo 5 lo pueda cumplir. Además, debe informar de las incidencias y correcciones adoptadas a la autoridad competente.

f) Deberán conservar los archivos de registro generados y permitirá su acceso a los estados miembros.

g) Deberán colaborar con las autoridades competentes proporcionando la información y documentación necesaria de su sistema.

3. Los programadores de AWS:

a) Deberán asegurarse de que el software no viola ningún derecho fundamental recogido en la regulación internacional.

b) Deberán informar a los proveedores de los sus posibles y potenciales fallos.

c) Tendrán prohibido ceder, recibiendo o no alguna compensación económica, el software de IA a terceros países no miembros de OTAN.

4. Los operadores de AWS:

a) Deberán emplear el AWS conforme a sus instrucciones de uso y a la misión encomendada.

b) Deberán asegurarse de que los datos de entrada sean correctos, completos y pertinentes de acuerdo a la finalidad del sistema.

c) Deberán supervisar constantemente el AWS y cuando considere que existen motivos justificados para que el AWS presente un fallo, informará al escalón superior y suspenderá la actividad del sistema.

d) Conservarán y mantendrán la confidencialidad de los archivos de registro generados.

Artículo 7. Autoridad de evaluación

1. Cada estado miembro designará una autoridad u organismo que será el encargado de realizar la validación del AWS conforme a las condiciones establecidas y cumpliendo con los requisitos del Artículo 5.
2. La autoridad u organismo encargado actuará de forma imparcial y objetiva sin que exista conflicto de interés entre ninguna parte.
3. La autoridad u organismo mantendrá la confidencialidad de la información y notificará del resultado de la evaluación a la autoridad designado por cada estado.
4. La autoridad u organismo contará con el suficiente personal especializado para realizar la evaluación.

Título IV. Medidas de apoyo al desarrollo de AWS

Artículo 8. Medidas de apoyo.

1. Los estados miembros facilitarán a los proveedores espacios controlados designados para el desarrollo, prueba y validación de los AWS.
2. Los proveedores y participantes del espacio controlado facilitado por cada estado responderán por los daños o perjuicios ocasionados a terceros durante el desarrollo del AWS.
3. Las actividades realizadas en el espacio controlado deberán ser autorizadas y coordinadas por el estado en el que tienen lugar.

Artículo 9. Tratamiento de datos en los espacios controlados para pruebas.

1. En el espacio controlado se tratará datos de carácter personal y debidamente autorizados con la finalidad de realizar el desarrollo y las pruebas de los AWS.
2. Los datos recogidos no serán empleados con fines distintos que el de realizar las pruebas y validación de los sistemas.
3. Los datos recopilados no serán transferidos de ninguna forma a terceros y tendrán la consideración de información confidencial.
4. Deberá existir un mecanismo para detectar posibles fugas de datos que pudieran vulnerar cualquier derecho fundamental u ocasionar perjuicio alguno a sus propietarios.
5. Una vez finalizadas las pruebas, los datos recopilados serán destruidos.

Título V. Gobernanza

Artículo 10. Comité de IA en OTAN

1. Se establece un Comité OTAN de IA (en adelante, el Comité).
2. El Comité asesorará y asistirá a los estados miembros a fin de garantizar la regulación existente en materia de AWS y coordinará los análisis pertinentes en caso de fallos del sistema, ya sean entre estados miembros o no.
3. El comité estará formado por autoridades representantes de cada país que deberán tener los suficientes conocimientos de IA y AWS a fin de comprender la importancia y el alcance de su responsabilidad.
4. Sin menosprecio de otras funciones que pudiera realizar, el Comité deberá:

a) Recopilar y compartir información tanto técnica como de funcionamiento entre los estados miembros con AWS.

b) Publicará recomendaciones, lecciones aprendidas y buenas prácticas en el empleo de AWS que deberán ser accesibles a todos los estados miembros.

Título VI. Base de datos para AWS

Artículo 11. Regulación base de datos de AWS.

1. Se creará una base de datos única y accesible para todos los países miembros y que será actualizada por aportaciones debidamente tratadas por cada estado.
2. No se permitirá la creación de bases de datos independientes.
3. Los proveedores podrán añadir información a la base de datos y tendrán acceso únicamente a aquella información de carácter público.
4. El Comité velará por el cumplimiento de las condiciones de la base de datos, auditando a cada estado miembro y estableciendo las sanciones administrativas que correspondan en caso de negligencia o incumplimiento.
5. Cada estado será responsable del mantenimiento de sus servidores conectados a la base de datos y responderá en caso de que estos queden expuestos.

Título VII. Código de Conducta

Artículo 12. Código de conducta.

1. Tanto el Comité como los estados miembros tomarán las medidas necesarias para que el AWS sea compatible con las políticas ambientales y de seguridad existentes, así como con los valores éticos y morales de la Organización.

Título VIII. Responsabilidad y Sanciones

Artículo 13. Responsabilidad

1. La responsabilidad de cada parte vendrá definida por la negligencia o incumplimiento de sus funciones. Se proponen una seria de sanciones para cada caso:
2. El proveedor tendrá responsabilidad civil en cuanto al incumpliendo de los deberes especificados en el Artículo 6.1. El incumplimiento de tales obligaciones podría acarrear una sanción administrativa de entre 500.000 a 20 millones de euros.
3. El programador tendrá responsabilidad penal en cuanto al incumpliendo de los deberes especificados en el Artículo 6.2. El incumplimiento de tales obligaciones podría acarrear una sanción entre 24 a 60 meses de prisión.
4. El operador tendrá responsabilidad penal en cuanto al incumpliendo de los deberes especificados en el Artículo 6.3. El incumplimiento de tales obligaciones podría acarrear una sanción entre 6 a 18 meses de prisión.
5. El mando asumirá responsabilidad por su propia condición de mando militar y responderá en función de la legislación ya existente de carácter internacional. Atribuyéndole únicamente responsabilidad por omisión según los Artículos 86 y 87 del Protocolo Adicional I (Comité Internacional de la Cruz Roja, 1977) y la norma 153 del Derecho Consuetudinario (Henckaerts and Doswald-Beck, 2007).

Artículo 14. Sanciones.

1. Cada estado miembro, de conformidad con esta propuesta, posee soberanía y podrá adoptar o no las sanciones propuestas en el Artículo 13. Sin menosprecio, en ningún caso, de tratar de compensar el perjuicio o daños causados a terceros mediante compensación económica. Para esta se tendrá en cuenta la gravedad y naturaleza de la infracción y de los daños causados.

7. CONCLUSIONES

A continuación, se exponen las conclusiones extraídas tras la finalización de este trabajo correspondientes al objetivo general y a cada objetivo específico:

1) Se ha propuesto la base para la creación de una regulación específica a nivel OTAN y centrada en el desarrollo de AWS como sistemas futuros de EW que se adapten a las capacidades que se requieren en los actuales y futuros teatros de operaciones. La regulación propuesta resuelve satisfactoriamente los principales problemas y lagunas legales existentes acerca de su empleo, alcance y determinación de responsabilidad.

2) Se ha trabajado y operado con equipos propios de EW de la Cía. de EW 1/II/31. Las entrevistas planteadas y las conversaciones informales con sus operadores a diario han permitido definir las principales capacidades de EW que posee España desplegadas en zona de operaciones. Estas son la interceptación, goniometría y obtención de información, ya sea por medios de radiofrecuencia, telefonía móvil o telefonía satélite.

3) Con la colaboración del Brigada Baña, miembro del CCAL del Regimiento de Guerra Electrónica Nº31, se ha comprobado que la llegada y empleo de AWS es una realidad cada vez más cercana. Se espera conseguir aeronaves RPAS con capacidad de análisis de imágenes y un sistema capaz de reconocer y traducir palabras claves en los diferentes idiomas y dialectos que se hablan en cada teatro de operaciones, con la que se podrían notificar alertas tempranas. Tanto en la aeronave RPAS como en el sistema de traducción se emplearía IA, ambos sistemas trabajarían de forma autónoma, lo que dotaría a la Cía. de EW 1/II/31 de mejores capacidades.

4) Se ha analizado la problemática acerca de la determinación de responsabilidades en sistemas que implementen IA. Se ha concluido que la determinación de estas es una tarea extremadamente compleja que requiere de conocimientos avanzados en la materia en la que intervienen numerosas partes, como proveedores, desarrolladores, programadores, operadores, mandos que autoricen su empleo, etc. Esta la razón de la actual carencia de una regulación específica sobre sistemas con IA y su lento desarrollo

5) Se ha analizado la jurisprudencia nacional e internacional sobre la responsabilidad del mando, comprobándose que no existe una regulación específica sobre esta en el empleo de medios de EW de ningún tipo. Respecto a la jurisprudencia acerca del uso de AWS y la responsabilidad del mando, tampoco existe una regulación específica. Se concluye que tanto nacional, como internacionalmente, al mando solo se le puede atribuir una responsabilidad por omisión o negligencia respecto a sus subordinados. En lo que respecta a la legalidad de AWS y medios de EW actuales, se aplicaría la jurisprudencia general existente referente a sistemas de armas.

6) Se han planteado tres supuestos casos de estudio, referentes a escuchas no autorizadas, fallo de un AWS y perturbación electrónica en diferentes situaciones. A partir de su análisis ha quedado patente que la jurisprudencia actual no es suficiente y no está actualizada a las situaciones que se pueden dar, especialmente, en el caso del AWS y de la perturbación electrónica.

7) Finalmente, se concluye que los dispositivos y sistemas de armas que implementen IA son una realidad y que, probablemente, la “Propuesta del Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión” (European Commission, 2021), pueda ser aprobada en un

futuro próximo. Sin embargo, esta propuesta no afecta al ámbito militar. De acuerdo a esto y como línea de acción futura se propone el desarrollo de una propuesta formal, en el ámbito de defensa, sobre el desarrollo, empleo, capacidades y responsabilidades en AWS. Además de una regulación, nacional al menos, respecto a la responsabilidad del mando en el empleo de medios de EW.

REFERENCIAS BIBLIOGRÁFICAS

A Definitivas (2022). Acuerdo de confidencialidad. Disponible en: https://adefinitivas.com/arbol-del-derecho/modelo-de-acuerdo-de-confidencialidad-a-definitivas/ [Consultado 10-09-2022].

Alpert, M. (2021). Segunda Guerra Mundial: ¿Pudo Hitler derrotar a Inglaterra con los misiles V-2? Disponible en: https://www.lavanguardia.com/historiayvida/historia-contemporanea/20210718/7601203/pudo-hitler-derrotar-inglaterra-misiles-v-2.html [Consultado 15-09-2022]

Cambridge University Press (2022). Cambridge Dictionary. Disponible en: https://dictionary.cambridge.org/ [Consultado 12-09-2022].

Comité Internacional de la Cruz Roja (1977). *Protocolo Adicional I.* Ginebra.

Corte Penal Internacional (1998). *Estatuto de Roma de la Corte Penal Internacional*. Roma.

Cortes Generales (1978). *Constitución Española*. Madrid.

Defense Innovation Board (2020). *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense Defense Innovation Board*. Washington.

European Commission (2021). *Proposal for a regulation of the european parliament and of the council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. Bruselas.

Gobierno de España (1981). *Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio.* Madrid.

Gobierno de España (1989). *Ley Orgánica 2/1989, de 13 de abril, Procesal Militar*. Madrid.

Gobierno de España (1995). *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*. Madrid.

Gobierno de España (2003). *Ley Orgánica 15/2003, de 25 de noviembre, por la que se modifica l a Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*. Madrid.

Gobierno de España (2011). *Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas*. Madrid.

Gobierno de España (2015). *Ley Orgánica 14/2015, de 14 de octubre , del Código Penal Militar*. Madrid. Available at: http://www.boe.es.

Henckaerts, J.-M. y Doswald-Beck, L. (2007). *El derecho internacional humanitario consuetudinario.* Buenos Aires.

Jeffrey H. Fischer (2022). *A Key Reason for Russia's Colossal Electronic Warfare Failure in Ukraine*, Disponible en: *https://www.thedefensepost.com/2022/04/13/russia-electronic-warfare-failure-ukraine/#go-to-content* [Consultado 10-09-2022].

Lobo Almazán, E. (2022). *Uso de la fuerza y responsabilidad del superior*. Trabajo Fin de Máster. Universidad de Granada.

Mando de Adiestramiento y Doctrina (2009). *ACART-VA-055 (Guerra Electrónica)*. Granada.

Ministerio de Defensa (2009). *Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas*. Madrid.

ANEXOS

1. Anexo I. Plantilla Orgánica Cía. de EW 1/II/31

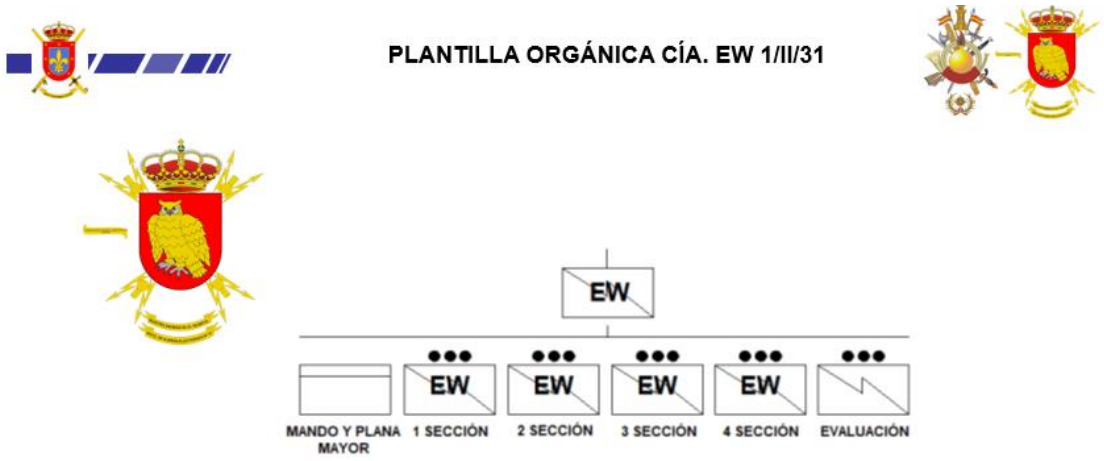

Imagen 2. Plantilla Orgánica. Fuente: Elaboración Propia

2. Anexo II. Acuerdo de Confidencialidad

Acuerdo de Confidencialidad

En Madrid, a __ de septiembre de 2022

De una parte, D./Dña. _____, mayor de edad, de nacionalidad española, con domicilio a estos efectos en _____ y con DNI núm. _____, en representación de _____. (en adelante la sociedad).

De otra parte, D./Dña. _____, mayor de edad, de nacionalidad española, con domicilio a estos efectos en _____ y con DNI núm. _____, en representación de _____ (en adelante la Parte).

MANIFIESTAN Y CONVIENEN

a)Que_____ _____es_____ _____ _____.

b)Que_____ _____es_____ _____ _____.

Que expresado cuanto antecede, las partes se comprometen y obligan, de forma expresa, a cuanto sigue:

Se han iniciado o están a punto de iniciarse conversaciones entre la sociedad y la Parte con el propósito de obtener información para realizar su Trabajo Final de Grado del Grado en Ingeniería en Organización Industrial de la Universidad de Zaragoza; y en relación con el propósito anterior, la sociedad podrá proporcionar a la Parte Información Confidencial

SE ACUERDA lo siguiente:

1.- En el presente Acuerdo, los términos que figuran a continuación tendrán el significado que les corresponde:

● Información *Confidencial*: significa que la información perteneciente a la sociedad y comunicada confidencialmente entre la sociedad y la Parte que no está o no ha entrado en el dominio público y no está disponible al público en general.

2.- La Parte acuerda lo siguiente:

2.1.- La Parte se compromete por la presente a que la sociedad:

2.1.1.- En ningún momento, sin el consentimiento previo por escrito de la sociedad, utilizará, divulgará o revelará ninguna Información Confidencial a ninguna persona o Parte y no enviará

ninguna Información Confidencial, ni hará que la misma sea enviada por correo, fax, teléfono, videoconferencia o correo electrónico o por cualquier otra forma de transmisión de datos que no sea de conformidad con los procedimientos de protección de datos de la sociedad o sin el consentimiento previo de la sociedad;

2.1.2.- Usar la Información Confidencial únicamente para el propósito descrito anteriormente, o para cualquier otro propósito, que la sociedad pueda acordar.

2.1.3.- Mantener una estricta confidencialidad con respecto a toda la Información Confidencial.

3.- El presente documento se interpretará y regulará en todo lo que no esté expresamente determinado conforme a la legislación española.

Las partes acuerdan someter cualquier cuestión relacionada con el presente Contrato a los Juzgados y Tribunales de Madrid, con renuncia expresa a sus fueros internos que les sean aplicables. El presente Contrato se regirá e interpretará de acuerdo con las leyes españolas.

Y en prueba de conformidad, firman el presente Acuerdo de confidencialidad a un solo efecto, en el lugar y fecha antes indicados.

Por _____ Por _____

3. Anexo III. Modelo de Entrevista

1 ¿Dónde está usted encuadrado dentro del Regimiento de Guerra Electrónica 31?

2 ¿Qué experiencia tiene en el empleo de medios de EW? Despliegue zona de operaciones, ejercicios…

3 ¿De qué capacidades dispone su compañía?

4 Desde su punto de vista, ¿qué capacidades son las que están demandando los actuales teatros de operaciones?

5 ¿Cuáles son las líneas de acción en la que están trabajando? ¿Qué capacidades se plantean implementar o mejorar?

6 ¿Cree que la implementación de IA en medios de EW podría otorgar nuevas y mejores capacidades? ¿Cuáles?

7 ¿Considera alguna otra capacidad importante o de interés para España que no se haya nombrado?

8 Desde su experiencia, ¿cuáles cree que son los potenciales impedimentos legales que pudiera haber en el empleo de medios de EW?

9 ¿Piensa que las nuevas tecnologías, como la IA pudiera cambiar el tratamiendo de responsabilidades en el empleo de medios de EW? ¿En qué manera?