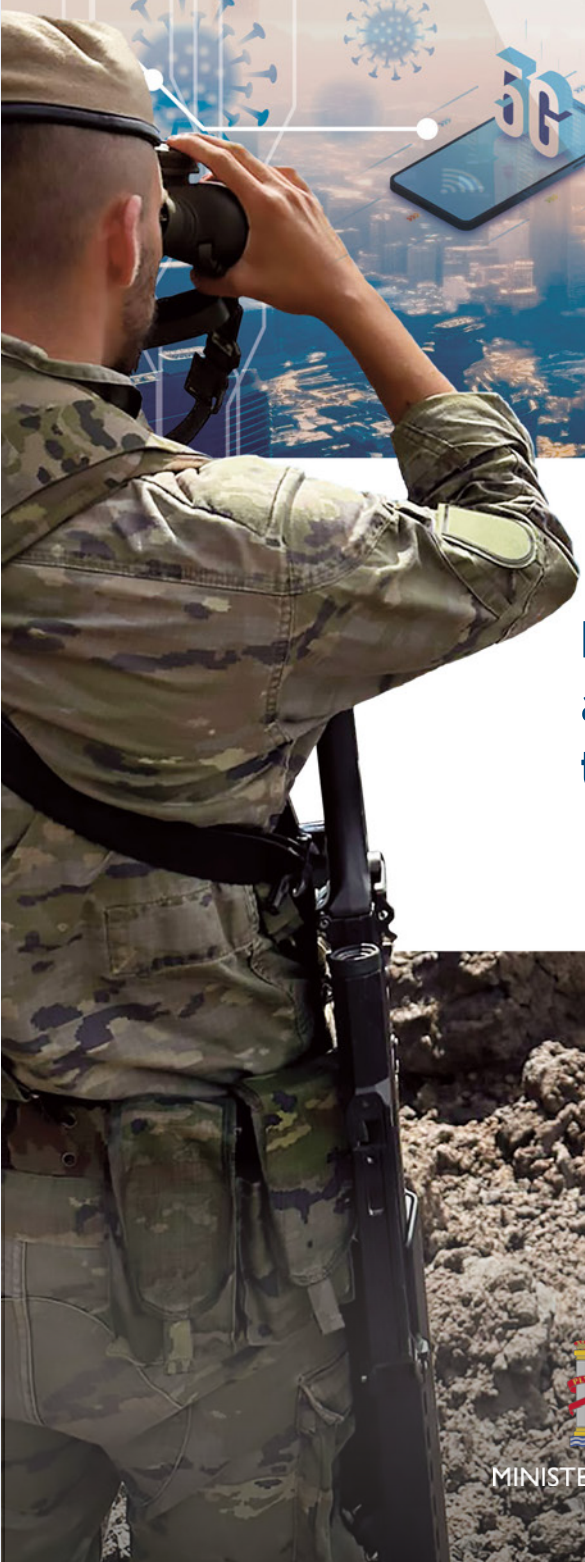
La Protección de la Fuerza ante las nuevas amenazas tecnológicas



MINISTERIO DE DEFENSA

La Protección de la Fuerza ante las nuevas amenazas tecnológicas

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de Defensa
https://publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

publicaciones.defensa.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

NIPO 083-23-239-8 (impresión bajo demanda)
ISBN 978-84-9091-826-5 (impresión bajo demanda)

NIPO 083-23-240-0 (edición en línea)

Depósito legal M 32001-2023
Fecha de edición: diciembre de 2023
Maqueta e imprime: Imprenta Ministerio de Defensa

En esta edición se ha utilizado papel procedente de bosques gestionados de forma sostenible y fuentes controladas.

ÍNDICE

Introducción

Luis Alberto Hernández García

La Protección de la Fuerza es un requisito indispensable para garantizar el cumplimiento de la misión en un entorno complejo, disputado y, ciertamente, peligroso. A los riesgos y amenazas tradicionales, que en general persisten (y no hay que descuidar), se unen los asociados al exponencial avance tecnológico, en las más variadas áreas del conocimiento científico. La tecnología, a su vez, genera nuevas vulnerabilidades en las fuerzas propias, susceptibles de ser explotadas por el adversario y con alto potencial de impacto.

La posesión de personal, medidas y medios adecuados para contrarrestar la amplia gama de funciones ligadas a la protección y a la seguridad; su adecuada gestión y dirección, de manera integrada, entre ellas y en las operaciones; el entendimiento tecnológico; la formación y la concienciación de todo el personal conforman un conjunto indivisible de requisitos para garantizar la Protección de la Fuerza y, por ende, la continuidad y la efectividad de las operaciones.

1. Objeto

El presente documento se enmarca en el Plan Anual de Investigación (PAI) del Centro Conjunto de Desarrollo de Conceptos (CCDC)[1] para el año 2023. Tiene por objeto poner de manifiesto cómo los avances tecnológicos afectan a la manera en la que se deben afrontar los riesgos y amenazas a la Fuerza, pues poseen la capacidad de potenciar la peligrosidad y efectos de los ya conocidos, al tiempo que crean otros inéditos hasta el momento. Solo mediante la correcta identificación, análisis y, sobre todo, actualización, de esos riesgos y amenazas será posible prevenirlos, detectarlos, frenar su ocurrencia y, en caso de que se materialicen, reaccionar e iniciar de

[1] Perteneciente a la División de Desarrollo de la Fuerza (DIVDEF) del Estado Mayor Conjunto (EMACON).

forma adecuada las correspondientes acciones de recuperación. Todo ello, a fin de garantizar la continuidad de las operaciones en un entorno operativo en el que la tecnología juega un papel predominante.

2. Desarrollo y estructura

Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases es el título de una obra de Alan Vick, publicada a mediados de la década de los noventa del pasado siglo y que, por aquel entonces, fue lectura imprescindible para los que se dedicaban a lo que se conocía como seguridad y defensa de bases aéreas, concepto extensible en general, a pesar de las particularidades de las diferentes dimensiones, a la protección de cualquier tipo de instalación, personal, equipo e información de carácter militar. Con una perspectiva básicamente aérea, la publicación ponía el énfasis en los ataques terrestres como principal riesgo a enfrentar a la hora de defender una base o aeródromo, una instalación militar.

Para comprender el fenómeno, el autor partía de la base del estudio de una variada casuística a nivel global, abarcando el periodo que va desde la Segunda Guerra Mundial (1940) hasta la Posguerra Fría (1992). Vick detectó en su investigación que la intención de los atacantes siempre podía categorizarse en el marco de alguno de los cuatro objetivos principales que definió, a saber: toma y captura del aeródromo atacado, privación de la posibilidad de uso del aeródromo, acoso a los defensores de las instalaciones y destrucción de aeronaves y equipo. En todo caso, el resultado pretendido por las fuerzas agresoras era siempre la disrupción de las operaciones.

También prestó atención a la evolución que los ataques habían sufrido a lo largo de los tiempos. Si en la Segunda Guerra Mundial buscaban la penetración a través de las defensas perimetrales, conflictos como el de Vietnam pusieron de manifiesto el valor del ataque desde la lejanía, usando armas de tipo *stand off* casi en el 100 % de las ocasiones. En cuanto a las deficiencias de los defensores, el libro considera que las principales fallas en la protección de las instalaciones militares siempre eran achacables a la falta de efectivos, medios o preparación. Por otra parte, ya en aquellos lejanos años noventa, el autor concedía especial importancia a la creatividad y la innovación como fuente de mejora de la protección. A este respecto, cita Vick, como ejemplo, la efectividad que tuvo en Vietnam el hecho de que la respuesta estadounidense a las agresiones de la parte vietnamita se realizara desde una perspectiva conjunta.

Antes de finalizar este breve repaso de la publicación citada, tan solo apuntar una de las cinco principales conclusiones que el autor extrae, la que afirma que, en el periodo estudiado, más de 2.000 aeronaves habían sido destruidas o dañadas en tierra y que, para conseguirlo, tan solo se precisó

de la acción de pequeñas fuerzas, las cuales emplearon la mayoría de las veces armas nada sofisticadas. El texto, como se ha dicho, de enfoque eminentemente aeronáutico, permitía no obstante extrapolar las conclusiones y enseñanzas principales a cualquier otro ámbito de las Fuerzas Armadas e incluso a organizaciones civiles.

Por aquel entonces, la seguridad de acuartelamientos militares, bases, buques o convoyes se encontraba muy enfocada a la protección física de instalaciones, equipos, personas o información en territorio nacional, frente a riesgos como atentados terroristas, sabotajes, espionaje, intrusiones, robos, emergencias internas, etc. Junto a esto, en el marco de la eclosión de las misiones en el exterior, se hacía patente la necesidad de protegerse también lejos del país de origen. Entre otros, tomaba forma en el ámbito internacional el pionero y sugerente concepto de «Survive To Operate» (STO)[2], de vocación principalmente expedicionaria.

En concreto, recibió un notable impulso en el ámbito aeronáutico, en el que estas tres palabras dejaban claro, por un lado, la necesidad de salir adelante para ser capaces de operar, esto es, de generar salidas para cumplir la misión asignada. No en vano, las operaciones aéreas necesitaban de una base kilométrica para albergar el inseparable complemento de la aeronave: una pista para tomas y despegues, con todas sus servidumbres aeronáuticas, que no se podía encontrar en cualquier lugar y, mucho menos, improvisar, dado su complejo diseño y funcionamiento. Por tanto, había que defenderla a toda costa frente a multiplicidad de riesgos y amenazas, pues era insustituible y su destrucción o inoperatividad suponían la denegación en tierra del Poder Aéreo, explotando así el adversario su principal fragilidad. Por otro lado, el concepto dejaba claro lo que suponía la protección, la seguridad, que no era sino un medio más, eso sí, necesario junto con otros, como era el caso de la logística, para garantizar la operatividad. Así, la protección no se concebía como un fin en sí misma, no como un obstáculo, sino como un elemento facilitador de la operatividad. La misión final predominaba indiscutiblemente sobre una de las funciones que la posibilitaban. Había que sobrevivir a la situación de agresión para poder operar; no había otra razón para hacerlo. De nuevo, por analogía, el concepto podía considerarse extrapolable a otros servicios y organizaciones.

Con el paso del tiempo, las funciones clásicas de seguridad, junto con conceptos como STO, evolucionaron y confluyeron en el marco aliado hacia otro más amplio, dinámico e inclusivo, por su vocación de aplicación conjunta, necesidad que ya observara Vick, aumentando además el espectro

[2] El concepto STO incluía todas las medidas de seguridad física, protección activa y pasiva, así como actividades de recuperación necesarias para garantizar la continuidad de la secuencia de generación de las operaciones.

de la protección más allá de lo que tradicionalmente se entendía por «seguridad» y «protección» en el plano físico. El concepto exportaba a su vez la función de protección a otros ámbitos de operación, como el ciberespacial o el cognitivo y buscaba una interacción más eficaz de todas las tareas relacionadas con la protección frente a todo tipo de riesgos, tanto en despliegues en el exterior como en territorio nacional. Además, contemplaba los conceptos de continuidad y gestión de las consecuencias en caso de ataque, emergencia o desastre de una forma más integral, más allá de las meras tareas de recuperación física de instalaciones esenciales.

Nacía el nuevo término, que permanece hoy en día para englobar todas las tareas citadas y que se conoce como «Protección de la Fuerza». La doctrina conjunta española[3] establece que esta función conjunta:

> «[...] engloba aquellas actividades que tienen como objeto minimizar la vulnerabilidad del personal, equipo, material, instalaciones, información, operaciones y actividades de la Fuerza y de los elementos no militares que apoyan, acompañan o están bajo responsabilidad de la Fuerza, frente a las acciones adversarias, propias, y frente a los riesgos sanitarios, naturales, tecnológicos y accidentes. Su finalidad es preservar la libertad de acción del Comandante y garantizar la operatividad de la Fuerza. La Protección de la Fuerza se materializa mediante la gestión del riesgo que concluye con la adopción de diversas medidas que contrarresten o mitiguen las amenazas procedentes del adversario y del entorno».

Asimismo, se incluye en este amplio concepto la referencia a cuatro aspectos esenciales al margen de la mera disposición de personal, sistemas o equipos especializados dedicados a las tareas de protección. Se trata de la adecuada gestión de los riesgos, que facilite la orientación y optimización del esfuerzo de protección; del necesario planeamiento, que defina requerimientos de capacidades y grados de disponibilidad en las diferentes situaciones y niveles de alerta, el que debe estar integrado en el planeamiento general de las operaciones; de la importancia del mando y control de la función en los diferentes niveles de mando, del estratégico al táctico y, finalmente, de la inclusión de los aspectos de la Protección de la Fuerza en el adiestramiento y certificación de unidades y estructuras conjuntas.

Sirva este breve repaso histórico-conceptual como base para el establecimiento de algunos paralelismos casi treinta años después, a fin de comprobar que, en un escenario muy distinto en cuanto a complejidad de las amenazas, medios, perfil del combatiente, tácticas, técnicas y

[3] Estado Mayor de la Defensa. (2019). *Protección de la Fuerza. PDC-3.14*. Madrid, Ministerio de Defensa. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/PDC-314_PROTECCION_DE_LA_FUERZA_para-web_09003a9980b53cd7.pdf

procedimientos, carácter del conflicto en general, algo permanece inmutable. Se trata de la intrínseca peligrosidad del entorno, que apunta a las infraestructuras, personas, operaciones, equipos e información, capacidades en general, como objetivos de excepción para denegar temporalmente o acabar con la operatividad de las fuerzas militares o de cualquier otro tipo de organización antes de ser capaces de actuar.

En efecto, se puede afirmar que la Fuerza se encuentra bajo una amenaza permanente, conformada por la confluencia de una gran diversidad de riesgos asociados a actores hostiles, no siempre de carácter estatal o de naturaleza militar, ni necesariamente externos a la propia organización. Dichos actores, muchas veces, no son ni siquiera reconocidos en primera instancia como potenciales adversarios o agresores y, además, se mueven con manifiesta ambigüedad en los nuevos ámbitos de operación no físicos, esto es, el ciberespacial y el cognitivo.

Esta amenaza se ve además potenciada por el exponencial avance tecnológico que, impulsado en los últimos tiempos a través de la iniciativa privada y los mercados e intereses comerciales civiles, se ha «democratizado» en lo que respecta a la accesibilidad del común. Este hecho sitúa la tecnología al alcance, no ya de cualquier estado, sino de todo aquel actor no estatal que pueda pagarla, la mayoría de las veces a un precio no muy alto, teniendo en cuenta la relación coste-beneficio. Además, la tecnología forma cada vez más parte intrínseca de las organizaciones, empleándose con profusión en todos sus sistemas, procesos, apoyos y relaciones, lo que abre nuevas brechas potenciales a la seguridad de sus bienes, intereses y operaciones.

El empleo de la tecnología posee la capacidad para multiplicar así el poder del intruso, del terrorista, del criminal, del pequeño grupo de operaciones especiales o de las armas de tipo *stand off*, en el papel de la «serpiente» a la que alude Vick, que amenaza el «nido». Ahora el atacante, amparado en la automatización, la lejanía, la velocidad de ejecución, la rapidez de cálculo, la letalidad, el volumen, la novedad, la ocultación, la ambigüedad de la atribución, etc., que proporcionan las diversas tecnologías, puede conseguir sus objetivos con niveles de riesgo mínimos, así como de acierto, precisión y poder de devastación hace unos años impensables. Como el ofidio, la «amenaza tecnológica» se adentra hacia su objetivo con sigilo, empleando la sorpresa, con extrema habilidad y, sobre todo, con grave peligro para la Fuerza, las operaciones y sus apoyos. De hecho, en el más alto nivel de la jerarquía documental, la Estrategia de Seguridad Nacional española (ESN 2021) destaca «el papel primordial de la tecnología en la mayoría de las amenazas».

Y son innumerables los frentes que abren las tecnologías innovadoras, emergentes y disruptivas (*Emerging and Disruptive Technologies*-EDT)

cuando se trata de proteger a la Fuerza, a la organización, así como a su actividad y operaciones. A pesar de los indudables beneficios del avance tecnológico, que admite poca cuestión si se mide en términos de creación de bienestar, riqueza y libertad para el ser humano, la tecnología en las manos equivocadas y con fines dañinos es un fenómeno que conviene vigilar y frente al que es necesario protegerse.

Por citar solo algunos ejemplos, la inteligencia artificial generativa viene probando, sobre todo recientemente, su enorme potencial para el engaño, la manipulación y la desinformación. La automatización de procesos permite además intensificar agresiones en cuanto a alcance, volumen e intensidad; la computación cuántica amenaza con acabar con la seguridad de la información tal y como la entendemos en la actualidad; la autonomía reduce el riesgo de exposición del atacante, siendo buena prueba de ello la proliferación exponencial del uso de drones en los conflictos armados más recientes. Por su parte, la fabricación aditiva facilita la logística del adversario, que gana en agilidad sin depender de complejos sistemas de soporte especializado; algunos metamateriales favorecen la ocultación y el *big data* o inteligencia de datos aumenta las capacidades del adversario en cuanto a obtención de información sobre nuestras potenciales vulnerabilidades.

Siguiendo con otros ejemplos, la energía dirigida posee un alto poder destructivo, aunque también incapacitante, en sus versiones no letales, muchas veces sin levantar sospecha de su uso por parte de un agresor; la biotecnología ayuda a optimizar, incluso a potenciar, capacidades humanas y promete revolucionar la guerra biológica. Las tecnologías espaciales, o las relacionadas con la inteligencia, vigilancia, adquisición de blancos y reconocimiento (*Intelligence, Surveillance, Target Acquisition, Reconnaisance*-ISTAR) permiten monitorizar posiciones y movimientos… y así hasta completar una interminable lista de posibilidades.

Al mismo tiempo, la elevada dependencia tecnológica de las actividades y servicios de las sociedades democráticas avanzadas; el consumo de equipos y servicios tecnológicos provistos por terceros, de afiliación no pocas veces incierta; la interconexión de equipos y sistemas empleando tecnología de redes en muchas ocasiones ajenas; incluso los nuevos usos sociales en los que la relación en línea de individuos y grupos es un hecho que coexiste, y que a veces se confunde, con la realidad, abren también potenciales brechas en la protección y la seguridad de las organizaciones, militares y civiles.

De hecho, la virtualización y la simulación pueden confundir percepciones; y las redes sociales y medios de comunicación, al margen de sus bondades e indudables beneficios, son un vector de posibilidades infinitas para la desinformación, la propaganda y la agitación. Los ciberataques, en cualquiera de

sus versiones y con diferentes objetivos, son ya parte del día a día de las organizaciones, que ven amenazada la operatividad y continuidad de sus complejos sistemas de gestión, incluidos los de seguridad y protección. El sencillo y familiar teléfono móvil, convertido ya en apéndice inseparable del individuo, abre ahora innumerables puertas de acceso a la organización, tantas como personas. Estos nuevos «puntos de entrada» ya no se blindan con capas de ningún material, ni se cierran con llave o candado, ni admiten un soldado o vigilante para controlar el acceso desde el exterior. Los medios para defenderlos son otros.

No obstante, continuando con la analogía que propicia el libro de Vick, hay que tener en cuenta que, en circunstancias en las que se trata de combatir el previsible ataque de una serpiente, la ansiedad o la parálisis frente a su presencia no son la solución. Muy al contrario, para poder mantenerlas a raya es necesario tener la mente despejada y será muy bueno conocer su hábitat, sus capacidades reales de hacer daño, las fortalezas y debilidades mutuas en esa situación, sus intenciones. No se trata ni de despreciar su poder dañino una vez alcanzan el nido ni, por supuesto, de caer en la ofidiofobia, sin más. Entender la tecnología y concienciarse de sus posibilidades es sin duda el primer paso para defenderse de su potencial para causar daño, intencionadamente o por negligencia. Como se ha citado, lo que defendiera Vick hace ya tres décadas con respecto a las deficiencias de los defensores, disponer de personal preparado, concienciado, medios adecuados y realizar una decidida apuesta por la innovación serán los principales recursos para garantizar una adecuada Protección de la Fuerza; una correcta seguridad de la organización.

Para continuar, es el momento de adentrarse en los diferentes capítulos que conforman esta obra. Ante la imposibilidad de dedicar con el formato disponible un capítulo a cada una de las tecnologías susceptibles de amenazar a la protección y la seguridad, se ha optado por escoger cuatro de ellas, consideradas por el grupo de trabajo como de alta representatividad. Su elección viene motivada por diversos factores, entre los que se incluye su relevancia y empleo en el momento actual, su nivel de desarrollo y accesibilidad, o su alto potencial dañino. El estudio de los cuatro aspectos tecnológicos que se exponen en los respectivos capítulos siguientes los completa un quinto, dedicado a los modelos de gestión, auténtica «clave de bóveda» de cualquier sistema de protección para la actuación integral frente a tales amenazas, que muchas veces no vendrán de forma aislada, sino en conjunción y, sin duda, se sumarán a las tradicionales, que persistirán.

Abre la obra el coronel Casildo Martínez Vázquez, del Ejército de Aire y del Espacio, con un primer capítulo dedicado al empleo de drones, capacidad omnipresente en los conflictos actuales, con el título «El desafío de

los Sistemas de Aeronaves No Tripuladas a la Protección de la Fuerza». Comienza el coronel Martínez con una revisión histórica del empleo de esta capacidad, resaltando su uso inicial como blanco aéreo, para destacar a continuación la rapidez con la que en los últimos tiempos se ha extendido su uso, tanto civil como militar, especialmente en relación con los de pequeño tamaño (sUAS - *small Unmanned Aerial System*), cada vez más fiables, baratos, potentes y versátiles, que se encuentran además al alcance de actores no estatales de variada naturaleza.

A esta circunstancia se une el hecho de su potencial combinación con otras tecnologías, como son la inteligencia artificial (IA) que, a la espera de que su evolución proporcione la autonomía absoluta, dota por el momento a los UAS de una mayor velocidad de respuesta; o la transmisión por redes 5G, clave para la operación remota a largas distancias y con múltiples terminales. Juntas, la IA y el 5G, son la clave para el futuro empleo de esta tecnología en modo «enjambre».

Continúa el autor afirmando que estos sistemas presentan la particularidad de que no son fácilmente detectables por los sistemas de Defensa Aérea empleados con éxito frente a las aeronaves tripuladas, por lo que constituyen una seria amenaza a la seguridad de instalaciones, equipos y personal.

Considera, por tanto, el coronel que es necesario dotarse de una capacidad integral para contrarrestarlos. Para neutralizar la amenaza, esta capacidad contra sUAS (C-sUAS) no habrá de limitarse al mero desarrollo de sistemas; sino que deberá además apoyarse en el empleo combinado de las capacidades existentes de Defensa Aérea y de Protección de la Fuerza, muchas de ellas ya probadas frente a otro tipo de amenazas tradicionales. Destaca algunas de estas capacidades, como son el dominio del área de responsabilidad en torno a la instalación; o las medidas de protección pasiva clásicas, como la ocultación, la dispersión, la decepción o el blindaje de estructuras de protección, aún útiles en gran medida, a pesar de los avances tecnológicos.

Finaliza el capítulo con una imprescindible referencia a la necesaria coordinación entre organismos nacionales para afrontar esta amenaza, especialmente con las Fuerzas y Cuerpos de Seguridad del Estado (FCSE); atreviéndose el autor a prever que los avances de los futuros sistemas C-sUAS no vendrán tan solo de la mano de nuevos y más avanzados sensores y efectores. Así, considera que la clave se encontrará en introducir cambios en la filosofía de empleo, apostando por una mayor autonomía que reduzca los tiempos de reacción ante una amenaza inminente y de alto potencial letal.

El segundo capítulo viene de la mano del coronel Claudio Sánchez Sánchez, del Ejército de Tierra. Pone de manifiesto que la no letalidad de un arma no la convierte automáticamente en menos peligrosa, lo que desarrolla bajo

el título «Protección contra la Capacidad No Letal». Relaciona el autor el empleo de este tipo de armas con los conflictos en la Zona Gris, esto es, con enfrentamientos por debajo del umbral del conflicto armado convencional en los que predomina el empleo de estrategias de tipo híbrido, la ambigüedad y, sobre todo, la contención de la escalada para no sobrepasar determinados límites que pudieran considerarse actos de guerra.

Une a esta circunstancia el hecho del, ya señalado, fácil acceso a la tecnología por la mayoría, de lo que se derivan a su juicio las dos principales razones para pensar que el uso de este tipo de armas va a suponer cada vez más una amenaza a la seguridad. Tras proporcionar una definición y determinar los principios que rigen la catalogación de las armas en esta categoría, desde ser capaz de disuadir hasta ser interoperables o fáciles de manejar, el autor se adentra en una taxonomía de los diferentes tipos, explicando sus principales características y proponiendo medidas para contrarrestar sus potenciales efectos en personas, sistemas e instalaciones.

Continúa el coronel hablando de las armas de control de masas, las más utilizadas y, por ende, desarrolladas. A pesar de su diseño inicial como defensa, es su presencia extendida lo que a su juicio las convierte también en potencial arma ofensiva de alto riesgo para la protección.

No obstante, cuando se trata de dañar objetivos a larga distancia, cree que el adversario podrá optar por las armas de energía dirigida (DEW - *Direct Energy Weapons*), que pueden ser letales o no letales, según el grado de su concentración. Se refiere a continuación el autor a los cuatro tipos principales, a saber: las armas láser, las de microondas o radiofrecuencia, las de haces de partículas y las sónicas. En relación con las segundas, describe su empleo en el interesante episodio vivido por personal estadounidense en la capital cubana, causante del conocido comúnmente como síndrome de la Habana. Tras un repaso por las armas biológicas y químicas, propone y explica un método de actuación que ve infalible para defenderse contra este tipo de armas, que es el aplicado también a las armas letales: «Que no te vean, que no te den, que no te maten».

Un tercer capítulo, «Impacto de la revolución Bio en la Protección de la Fuerza», del que se hace cargo el coronel Alberto Cique Moya, del Cuerpo Militar de Sanidad, refleja los aspectos relacionados con la biotecnología y la amenaza que supone a la protección. Se encuentra ya en marcha la que muchos consideran como la siguiente gran «revolución tecnológica» por producirse, una vez se vea culminada la correspondiente a las tecnologías de la información y las comunicaciones.

Así, sostiene el coronel desde el primer momento que la biotecnología, la biología sintética o la inteligencia artificial, aplicadas con fines ilícitos, incrementarán las amenazas a la protección.

Tras un breve repaso histórico de la presencia de armas biológicas y también químicas en la guerra, alerta el autor sobre un asunto de especial importancia por su novedad, que es el relativo al potencial uso de agentes biológicos o químicos para alterar los procesos cognitivos, más allá de la aplicación de las técnicas de neurociencia o neurotecnología. Se adentra a continuación a explorar las señales de la revolución «bio» en curso, resaltando a China como uno de sus principales impulsores a nivel global. Prosigue en este sentido el coronel con un llamamiento a la necesidad de potenciar los controles internacionales respecto a las armas químicas y biológicas. El fácil acceso a este tipo de armas requiere establecer una estrategia de *biopreparación* y *biorrespuesta* para proteger en todo momento al combatiente.

A continuación, el autor entra de forma más específica en los peligros derivados de la biotecnología y su exponencial desarrollo. Así, el documento trata el empleo de armas biológicas binarias, la integración de genes de diseño en el genoma de agentes biológicos, la creación de virus silentes, la ampliación de la gama de potenciales hospedadores del agente patógeno o el desarrollo de agentes biológicos de diseño.

Tras repasar de forma general los grandes desafíos que presenta la ingeniería genética, el coronel Cique finaliza proponiendo una serie de medidas para reducir riesgos y amenazas frente a este fenómeno. Para ello, habrá que potenciar la bioseguridad, no solo en las instalaciones militares, sino también desde el punto de vista de la cultura de la organización, de la investigación y el desarrollo de capacidades o mediante la vigilancia y la sospecha constantes.

El cuarto capítulo se reserva para la amenaza que supone a la seguridad el uso de los omnipresentes dispositivos móviles personales, de los que muchas personas poseen varios a la vez. Con él, el documento se adentra de lleno en la última de las extensiones del campo de batalla, esto es, el ámbito de operación cognitivo. Lo desarrolla el capitán de fragata José Ángel Tortosa Delfa con el título «Dispositivos móviles personales: riesgos multidominio en la palma de la mano».

El capitán de fragata Tortosa nos advierte de que los dispositivos electrónicos móviles personales, referidos a lo largo del texto con el acrónimo PED (del inglés *Portable Electronic Devices*) están llamados a ocupar una posición preferente entre todos los dispositivos tecnológicos usados en la actualidad. El aumento de la conectividad, la miniaturización de componentes, el incremento de su capacidad de procesamiento, su uso permanente o sus múltiples posibilidades de captación de datos (sensorización) son tendencias que confluyen en esa dirección.

El autor analiza su repercusión con respecto a la Protección de la Fuerza desde varios puntos de vista, teniendo en cuenta que el ámbito de operación

terrestre es seguramente el más proclive a sufrir el riesgo derivado del uso de los PED, al ser el que alberga con mucha diferencia el mayor número de interacciones humanas por estos medios. En su análisis de cómo el uso de PED afectará a la Protección de la Fuerza, el capitán de fragata tiene en cuenta aspectos como son las observaciones en conflictos recientes, como el de Ucrania, o las diferencias generacionales a la hora del uso de los dispositivos personales.

Considera el autor que el uso de PED va a afectar a la manera en la que tanto las fuerzas propias como el adversario emplean las capacidades. Alerta además de que, llegado el caso, pueden constituir una puerta abierta que proporcione este último acceso a nuestros datos y sistemas; todo ello, sin olvidar su potencial como elemento de transmisión, de desinformación y de acción de las operaciones de influencia en general. Por todo esto, los PED deben constituir un objeto de la protección en sí mismo.

El capitán de fragata Tortosa aporta varias potenciales soluciones sobre las diferentes posibilidades para gestionar este tipo de riesgos. La formación, la concienciación y el entendimiento tecnológico son, sin duda, opciones que se convierten en ineludibles para afrontar los riesgos en este aspecto. Considera además que, a pesar de lo que la intuición pueda indicar, las prohibiciones de uso de estos dispositivos no son solución con carácter general, ya que podrían acarrear consecuencias indeseadas, las cuales incluso agravarían el problema. Así, a la pérdida de determinadas funciones técnicas, se podrían unir la pérdida de motivación o moral por la desconexión, la falta de confianza institucional o la proliferación de dispositivos irregulares.

Finaliza la obra con el imprescindible capítulo dedicado a la gestión integral de la protección. En este quinto capítulo, «Dirección y gestión de seguridad frente a nuevas amenazas tecnológicas», el consejero de seguridad internacional José Luis Bolaños Ventosa, ofrece una visión sobre cómo afrontar este importante desafío desde un punto de vista del experto civil, del que bien se pueden identificar enseñanzas para la protección extrapolables al ámbito militar.

Resalta que el desarrollo tecnológico de los últimos años, a pesar del indiscutible avance social que ha propiciado, lleva aparejado un importante aumento de los riesgos digitales, los cuales han aumentado en frecuencia, impacto y potenciales consecuencias. La adecuada gestión y dirección de este entorno es esencial para garantizar la continuidad de las actividades propias de cualquier organización.

Para no dejar nada fuera, el autor estructura su capítulo en la exposición de dos modelos diferentes de gestión de la protección, aplicados especialmente en el ámbito de la organización civil. Completa su intervención en el documento con un caso de estudio de una empresa de infraestructuras críticas del sector de la energía.

El primero de ellos es el Modelo de Protección de Infraestructuras Críticas (PIC), que se recoge en una directiva europea del Consejo y que incluye una propuesta de modelo colaborativo e integrado con la intención de servir de referencia a los Estados miembros y a las empresas operadoras de los servicios esenciales en el ámbito de la Unión Europea. Como particularidad, reseña que el modelo apuesta, por primera vez, por la gestión integrada de riesgos físicos tradicionales y cibernéticos.

El segundo, de carácter internacional y visión global, es el modelo *Enterprise Security Risk Management* (ESRM), el que propone que la gestión de la seguridad se alinee con la estrategia general y objetivos de la empresa. Con un enfoque basado eminentemente en la gestión del riesgo, tiene en consideración el tratamiento integral de todos aquellos peligros aplicables a cualquier rama de la seguridad, sea física, cibernética, antifraude, de gestión de crisis o de continuidad de negocio.

El autor se centra con posterioridad en la descripción del caso práctico de implantación de un modelo de Seguridad Global en una multinacional del sector de la energía con infraestructuras críticas en diferentes regiones, incluyendo zonas de alto riesgo. Finaliza el autor con unas conclusiones aplicables a todos los nuevos modelos de gestión, que coinciden siempre en la necesidad de aproximaciones holísticas en el marco general de la organización, contemplando al unísono todos los aspectos de la seguridad, la necesidad de colaboración entre todos los actores implicados y la potenciación, tanto de la Inteligencia como de la formación del personal.

Concluido el repaso por los diferentes capítulos, queda solo reseñar que todo lo expuesto en el presente documento se considera que es, o puede ser aplicable, de una u otra forma, siempre con las pertinentes adecuaciones y, en su caso, excepciones, a cualquier tipo de organización, sea esta militar o civil, se encuentre en Territorio Nacional (TN), desplegada o expatriada, en un asentamiento fijo o en movimiento.

Para ello, será sin duda un objetivo primordial para las organizaciones contar con la adecuada protección que garantice su continuidad, buscando, como expresaba el viejo concepto, la manera de «Sobrevivir» para poder «Operar», al ritmo, con la agilidad y eficacia que los tiempos actuales demandan, en un entorno peligroso, complejo, disputado, ambiguo, incierto y, sobre todo, no lo olvidemos, tecnológico.

3. Agradecimientos

Para despedir esta introducción, quisiera agradecer en primer lugar el gran trabajo realizado por los autores de los diferentes capítulos. Su extenso conocimiento de los asuntos tratados, experiencia y, sobre todo,

dedicación durante los pasados meses, han sido un factor clave para el éxito de la obra. Con ella, contribuyen decisivamente a impulsar la necesaria Transformación de las Fuerzas Armadas en los más variados aspectos para afrontar con garantías el entorno operativo venidero.

Mención especial merece el CF Fernando Riaño Echanove, secretario del grupo de trabajo, que con su rigor, paciencia, método y constancia ha sabido realizar con gran maestría las necesarias tareas de coordinación y administración del equipo, conducentes a la publicación que tiene ante usted.

Muchas gracias finalmente al lector, pues sin él la obra no tendría ningún sentido, quedando todos los integrantes del grupo de trabajo a la espera de que sea de su agrado y pueda servir a sus expectativas y necesidades.

Capítulo 1

El desafío de los Sistemas de Aeronaves No Tripuladas a la Protección de la Fuerza

Casildo Luis Martínez Vázquez

Resumen

Como hemos podido observar en los conflictos recientes, la posesión y utilización de sistemas de aeronaves no tripuladas (UAS) se ha extendido entre un número cada vez mayor de actores estatales, no estatales y organizaciones terroristas, proporcionándolas capacidades inherentes al Poder Aéreo, que antes solo estaban limitadas a un reducido grupo de grandes potencias militares.

Entre estos sistemas, destaca la proliferación de los denominados *Low Slow and Small* UAS (LSS) o *Small* UAS (sUAS). Su potencial empleo hostil, o mal intencionado, supone una amenaza real y creciente para la seguridad de nuestras Fuerzas Armadas, así como para el resto de nuestra sociedad, al actuar fuera del umbral de detección de los sistemas de Defensa Aérea tradicionales.

Por ello, se analizará la evolución de estos sistemas y de sus tácticas de empleo, así como la necesidad de implementar una capacidad para hacerles frente y neutralizarlos. Esta nueva capacidad no se basa exclusivamente en la operación de nuevos sistemas diseñados para combatirla, sino también en la adaptación de otras medidas y capacidades existentes y ya probadas, como puede ser las incluidas en el ámbito de Protección de la Fuerza.

Palabras clave

Sistemas de Aeronaves No Tripuladas, Protección de la Fuerza, Defensa aérea, Capa baja, Evolución, Enjambre, Tecnología 5G, Inteligencia artificial.

The challenge of Unmanned Aircraft Systems to Force Protection

Abstract

As we have seen in recent conflicts, the possession and use of Unmanned Aircraft Systems (UAS) has spread among an increasing number of state, non-state actors and terrorist organizations, providing them with inherent air power capabilities previously limited to a small group of major military powers.

Among these systems, the proliferation of so-called Low Slow and Small *UAS (LSS) or* Small *UAS (sUAS) stands out. Their potential hostile or malicious employment poses a real and growing threat to the security of our armed forces, as well as to the rest of our society, as they operate outside the detection umbrella of traditional Air Defense systems.*

For this reason, the evolution of these systems and their tactics will be analyzed, as well as the need to implement a capability to face and neutralize them. This new capability is not only based on the operation of new systems specifically designed to counter it, but also on the adaptation of other existing and proven measures and capabilities, such as those included in the Force Protection area.

Keywords

Unmanned Aircraft Systems, Force Protection, Air Defense, Low Tier, Evolution, Swarm, 5G, Artificial Intelligence.

1. Introducción

Diseñados, inicialmente, como blancos aéreos para ejercicios de tiro, los cielos de Vietnam fueron testigos del bautismo de fuego de los sistemas de aeronaves no tripuladas (UAS) por parte de la Fuerza Aérea de EE. UU. (USAF), en 1964[1], donde realizaron misiones de reconocimiento, localización de objetivos y apoyo de guerra electrónica. Pocos años después, aprovechando parte de las enseñanzas obtenidas en las operaciones aéreas de la guerra de Yom Kippur, fue la Fuerza Aérea de Israel quien lo empleó en la operación Paz en Galilea, en junio de 1982, destruyendo en una única acción las baterías de misiles superficie-aire sirias desplegadas en el Valle de la Bekaa, mediante el empleo combinado de aeronaves tripuladas y UAS. En esta acción, los UAS actuaron como señuelos, lo que hizo posible que el ataque se ejecutara sin registrar ningún derribo de los cazabombarderos atacantes.

Al finalizar la Guerra Fría, la tecnología de los UAS continuó consolidándose. Desde 1995, los primeros *Predator* de la USAF empezaron a efectuar misiones de Inteligencia, Vigilancia y Reconocimiento (ISR) de manera permanente sobre los Balcanes y otras zonas del mundo, lo que constituyó el primer paso en el desarrollo de las tácticas con las que estos sistemas son empleados hoy en cualquier conflicto. No fue hasta 2001, tras los atentados terroristas de Nueva York, cuando los UAS empezaron a utilizarse en misiones de ataque con armamento guiado, tanto en operaciones antiterroristas como en misiones de apoyo aéreo cercano (CAS) a las fuerzas desplegadas en Afganistán y, luego en Irak.

Este periodo de tiempo, conocido como la *First Drone Age* (Rogers, 2022), se ha caracterizado por el monopolio en el uso de estos UAS armados en manos de un reducido grupo de potencias, principalmente EE. UU. Disfrutando de una incontestable superioridad aérea, los UAS operaban sin ningún tipo de oposición en cualquier lugar del planeta donde sus intereses lo demandasen, sin que esto implicase que estas fueran zonas con conflictos activos o que en ellas hubiera contingentes de tropas aliadas sobre el terreno.

Sin embargo, durante los últimos diez años, hemos podido observar como la situación ha ido cambiando y, además, no en la dirección deseada. La

[1] La USAF empleó el Lightning Bug en misiones de reconocimiento, tanto a gran altura como a baja cota, localización de objetivos, en especial asentamientos de baterías de misiles superficie-aire, y guerra electrónica (ESM). Desarrollado a partir de un blanco aéreo, el Firebee, realizó un total de 3.435 salidas entre 1964 y 1975, llegando a existir una versión capaz de lanzar misiles aire-superficie, anti-radiación y bombas guiadas, que, finalmente, no entró en servicio. Lanzados desde C-130 Hércules modificados, la aeronave desplegaba un paracaídas tras finalizar su vuelo, siendo recogido por un helicóptero.

posesión y uso de UAS se ha generalizado entre un número cada vez mayor de naciones, grupos no estatales hostiles y organizaciones terroristas, proporcionándoles capacidades inherentes al Poder Aéreo, que antes solo estaban limitadas a un reducido grupo de grandes potencias militares, a un coste muy inferior.

Esto se ha puesto manifiesto con el papel relevante de los UAS en todos los conflictos recientes, como ha sido el caso de las operaciones contra el ISIS en Irak, los conflictos civiles de Libia y Siria, la 2.ª guerra de Nagorno Karabaj, los ataques de Hezbollah y Hamas contra Israel o de los rebeldes hutíes yemeníes contra Arabia Saudí y Emiratos Árabes Unidos.

Esta *Second Drone Age* (Rogers, 2021) también se ha caracterizado por la proliferación de los inicialmente denominados *Low Slow and Small* UAS (LSS) o *Small* UAS (sUAS)[2], tanto en el ámbito civil como militar, con un cada vez mayor y más diverso número de aplicaciones, dado su enorme potencial. Por desgracia, su evolución tecnológica y la mejora de sus capacidades (en lo que respecta a sus sensores, carga de pago, comunicaciones y autonomía), su coste reducido y su fácil accesibilidad les han convertido en un arma de primera elección para actores no estatales y grupos terroristas.

Por primera vez, la tercera dimensión se encuentra también disponible para estas organizaciones. Y como ya hicieron en el pasado con los artefactos explosivos improvisados (IED), buscan seguir aprovechando las debilidades de sus oponentes, habiendo pasado de ser blancos de este tipo de ataques a tener la capacidad para llevarlos a cabo, no solo contra las fuerzas desplegadas, sino también contra diferentes objetivos situados dentro de nuestras fronteras (bases e instalaciones militares, infraestructuras críticas, edificios oficiales de gran valor y acontecimientos de elevada visibilidad o gran impacto mediático y psicológico). Además, es interesante resaltar su interés para mostrar públicamente que disponen de este tipo de sistemas y que poseen además un nivel avanzado en su empleo, como parte fundamental de sus campañas de propaganda y captación de personal (Veilleux-Lepage y Archambault, 2022).

Pese a ello, la amenaza planteada por el posible uso hostil de sUAS por grupos no estatales y organizaciones terroristas no se ha materializado hasta hace poco tiempo. Hezbollah comenzó a operar este tipo de aeronaves desde 2004, en misiones ISR sobre Israel y posteriormente Hamas siguió sus pasos, contando ambas con apoyo iraní. No fue hasta 2017 cuando se produjo el primer ataque con sUAS por parte de una organización de estas características, correspondiendo este dudoso honor al Estado Islámico (EI)

[2] De acuerdo con la clasificación OTAN, los sUAS son UAS clase I cuyo peso no supera los 150 kg, incluyéndose sistemas micro, mini y pequeños dentro de esta categoría.

durante las operaciones de reconquista de la entonces capital del califato, Mosul, por parte de las fuerzas iraquíes y de la coalición liderada por los EE. UU. (Chávez y Sweed, 2020).

Considerada la primera guerra de alta intensidad en la que ambas partes han utilizado una gran variedad de UAS de todo tipo y seguirán haciéndolo en el futuro, el conflicto entre Rusia y Ucrania de 2022-2023 ha puesto de manifiesto que estos sistemas son necesarios, pero no suficientes, para alcanzar la victoria en el campo de batalla. Los grandes UAS no has sido tan relevantes, a diferencia de lo ocurrido en los conflictos mencionados antes, dado que, cuando operan sin contar con superioridad aérea, son muy vulnerables a los sistemas de defensa aérea basados en superficie y a las acciones de guerra electrónica.

Por el contrario, han sido los sUAS y las municiones merodeadoras (*Loitering Munitions*, LM) quienes han adquirido un gran protagonismo, utilizándose de forma masiva a lo largo y ancho del campo de batalla desde el inicio de las hostilidades. Los sUAS, principalmente de origen comercial, han destacado por mejorar la precisión de los fuegos de artillería y reducir los tiempos críticos del ciclo de *targeting*, realizar misiones de ataque directo contra diferentes tipos de objetivos, así como por incrementar las capacidades de los combatientes de ambos bandos al nivel orgánico más bajo posible, al proporcionarles un conocimiento de la situación próxima del que antes carecían y que ahora contribuye a mejorar su supervivencia.

2. Lo pequeño está de moda: la evolución de la amenaza de los sUAS

Los sUAS se caracterizan por su reducida superficie equivalente radar (RCS) y por su baja firma infrarroja y acústica, lo que, unido a su altura de vuelo y su baja velocidad, les sitúan fuera del umbral de detección de los Sistemas de Defensa Aérea (SDA) en servicio hoy en día, ocurriendo lo mismo con los sensores que conforman el sistema de gestión del tráfico aéreo civil. Esta baja detectabilidad, junto a su dependencia de la conectividad, son las principales características que los diferencian de las aeronaves tripuladas y originan los principales problemas para ser gestionadas por el tradicional sistema de vigilancia y control aéreo.

Su constante evolución está haciendo que su uso se extienda rápidamente no solo en el ámbito militar, sino también en el civil, mediante sUAS más potentes y versátiles, con una mayor fiabilidad, que proporcionan mejores prestaciones a precios cada vez más reducidos, como consecuencia del abaratamiento de una tecnología avanzada de fácil uso y cada vez más accesible.

Desgraciadamente, esto ha hecho posible que actores no estatales y grupos terroristas hayan podido disponer de sUAS, principalmente de origen civil, para llevar a cabo acciones letales con gran efectividad y una baja exposición contra las fuerzas propias y aliadas desplegadas en el exterior, así como posibilitar que puedan utilizarse contra distintos tipos de objetivos situados en territorio nacional.

Además, estos actores son tremendamente innovadores para identificar y adaptar nuevas tecnologías en su beneficio, pudiendo tener capacidad para modificar sUAS de tipo comercial para ajustarlos a sus necesidades, e incluso fabricarlos de manera local. Para ello, han podido contar con el apoyo de determinados países, como pueda ser Irán, en el caso de Hezbollah, Hamas o los rebeldes hutíes (Rogers, 2023), o llevarlo a cabo sin ningún tipo de respaldo, como sucedió con el EI, que estableció una estructura centralizada que controlaba todos los aspectos relacionados con la producción y operación de este tipo de sistemas (Rassler, 2018).

Sin embargo, este espíritu innovador no es exclusivo de este tipo de organizaciones. Y una vez más, el ejemplo lo tenemos en Ucrania. Tras el conflicto separatista del Donbass y la anexión de Crimea por parte de Rusia, en 2014 se fundó Aerorovzvidka. Esta organización no gubernamental, integrada en las fuerzas armadas ucranianas, ha tenido desde su nacimiento un papel fundamental en el desarrollo y consolidación de la capacidad de reconocimiento aéreo mediante sUAS comerciales, incluyendo la fabricación de diferentes nuevos modelos, e incluso de un *software* de C2, Delta, a través de la integración de los datos proporcionados por los sUAS y otros sensores (Thomas, 2022).

Los sUAS continúan evolucionando para aumentar sus capacidades y reducir sus vulnerabilidades. Si bien la tendencia es que se reduzca tanto el peso como el tamaño de la aeronave, sus prestaciones no se verán afectadas, sino que se verán incrementadas en lo que afecta a su carga útil, velocidad, alcance y persistencia.

Al hablar de su evolución, parece razonable pensar que el principal motor de estas innovaciones venga de la mano de la inteligencia artificial (IA), que podrá llegar a convertir a estos sistemas en autónomos en el futuro. Sin embargo, en estos momentos, lo que hace realmente importante a la IA es su capacidad para realizar tareas a velocidades superiores a las que pueden ser hechas por los seres humanos (Boyle, 2020).

Otro aspecto importante de este proceso está dirigido a reducir aún más su ya de por sí baja detectabilidad. Aparte de posibles modificaciones en la forma y el tamaño del fuselaje de la aeronave y el uso de nuevos materiales en su fabricación, dirigidos a aumentar su furtividad, aunque puede llegar a incrementar sus costes, el objetivo principal será reducir las emisiones

electrónicas asociadas a los sUAS para dificultar su detección, seguimiento e identificación por parte de los sistemas C-sUAS.

Entre las técnicas utilizadas para ello podemos citar el uso de bandas de frecuencia diversas, la instalación de módulos de agilidad de frecuencias, el uso de tecnología 5G, que les hacen también más difíciles de ser discriminados (sobre todo en entornos urbanos), o bien, dotarles de sistemas de navegación (con sistemas inerciales o de reconocimiento del terreno) que les permita hacerlo de manera autónoma, sin conexión con el operador y sin dejar rastro de radiofrecuencia (RF) detectable (DSN, 2022).

En lo que respecta a la conectividad, la tecnología 5G proporcionará una cobertura casi total y la posibilidad de vuelo de los sUAS más allá de la línea de visión (BLOS), antes posible solo por comunicaciones vía satélite, especialmente en áreas urbanas, donde estará garantizada una conexión inalámbrica ininterrumpida a internet. Esto supondrá un gran cambio, al no requerir la operación del sUAS que el piloto tenga que estar en las proximidades del objetivo, lo que significa que el riesgo para estos se reduzca de manera considerable. Esta tecnología aumenta además exponencialmente la capacidad de interconectividad, al permitir la conexión de hasta un millón de usuarios en 1 km^2, posibilitando así la sensorización del campo de batalla, con todos los elementos conectados a una misma red e intercambiando la misma información. Asimismo, proporcionará velocidades de transmisión de datos que posibilitará la transferencia de datos y vídeo en tiempo real, reduciendo la latencias a menos de 1 m, garantizando que los dispositivos permanecerán conectados independientemente de su velocidad (Mackenzie y Kanellos, 2021).

Esta evolución también se traduce en su concepto de empleo y en las tácticas, técnicas y procedimientos (TTP) asociadas, principalmente en lo que respecta al empleo de numerosos sUAS en ataques múltiples y en enjambres (Kallenborn, Ackerman y Bleek, 2022), que, con carácter general, buscan saturar las defensas del objetivo a batir mediante la superioridad numérica de los atacantes, utilizando para ello sUAS desechables. Los ataques múltiples se basan en el uso de varios sUAS desechables que operan de manera simultánea contra un mismo objetivo, habitualmente con diferentes ejes de aproximación. Cada uno de estos sistemas es controlado individualmente, o pueden ser programados para que sigan una ruta programada mediante puntos de referencia (*waypoints*), sin que haya ningún tipo de enlace de datos entre cada aeronave, aunque sí podría haberlo, lógicamente, entre los distintos pilotos de los sUAS que intervienen en la operación.

Concebidos para operar de forma autónoma, sin control humano directo, todos los sUAS que operan en un enjambre, tanto de tipo cooperativo

como coordinado[3], estarán interconectados, compartiendo la información de sus sensores, tomando decisiones colectivas basadas en la IA y coordinando sus acciones para alcanzar sus objetivos. De esta manera, algunos de estos sUAS se encargarían de localizar los objetivos, mientras que otros actuarían como señuelos o perturbando sensores y equipos de comunicaciones, atacando los blancos asignados, verificando si estos han sido alcanzados y destruidos, reatacando otros objetivos... sin olvidar que también serían capaces de reaccionar ante las amenazas detectadas sin intervención humana, maniobrando, cambiando de rumbo, velocidad o altitud (Bowden, 2022).

La evolución tecnológica de los enjambres se ha visto potenciada por las capacidades proporcionadas por las redes 5G y la IA y todo apunta a que, antes de la próxima década, las principales potencias militares ya operarán este tipo de sistemas, si bien no parece previsible que ocurra lo mismo con los actores no estatales y organizaciones terroristas, incluso en el caso de aquellos que cuentan con apoyo exterior. De hecho, Israel ya los ha empleado contra Hamas en 2021 en el marco de la operación Guardián de las Murallas, con la misión de localizar y atacar a los terroristas que disparaban cohetes contra su territorio antes de que pudieran escapar, e incluso antes de que pudieran iniciar el lanzamiento (Antebi, 2022).

Sin embargo, no ocurre lo mismo con los ataques múltiples, dado que hay constancia de que estas organizaciones ya los han ejecutado, aunque sea de manera rudimentaria. Así, en 2018, grupos opositores al régimen de Bashar al-Assad atacaron con éxito la víspera del día de Año Nuevo a las fuerzas rusas desplegadas en la base aérea de Jmeimim mediante un ataque de ocho sUAS, dañando siete aeronaves y matando a dos militares rusos, aunque posteriormente las autoridades rusas declararon que el ataque había sido realizado con morteros (Watling y Waters, 2019). Posteriormente, esta base aérea volvió a ser atacada, junto a la base naval de Tartús, el día 5 de enero, por un total de trece sUAS, aunque en esta ocasión, todos fueron derribados (Bari Urcosta, 2020). Además, conviene recordar que estas organizaciones pueden incrementar aún más la letalidad de estos ataques cuando los combinan con el lanzamiento de otros tipos de armamento del que disponen, como pueden ser cohetes o granadas de mortero, o incluso, cuando los coordinan con intrusiones y acciones directas realizadas por sus combatientes en superficie, no debiendo descartarse que, en este tipo de acciones puedan llegar a ser empleados como señuelos para enmascarar su esfuerzo principal.

[3] Los enjambres son cooperativos cuando todos sus componentes operan como una sola unidad para realizar una única función, siendo de tipo coordinado si sus integrantes desarrollan tareas separadas y distintas, en coordinación entre sí.

La munición merodeadora (LM) ha adquirido una gran notoriedad a lo largo de la última década, en especial en la guerra de Ucrania, donde han sido utilizadas ampliamente por ambos bandos. A pesar de que son conocidas de manera vulgar como drones suicidas o kamikazes, es importante recordar que estos sistemas de armas no son UAS, sino munición en sí mismos, encuadrándose entre los misiles de crucero y los UAS de combate, compartiendo características de ambos (Bode y Watts, 2023). La principal diferencia que tienen con los misiles de crucero es que estos no pueden orbitar o sobrevolar la zona donde se encuentra el objetivo asignado durante mucho tiempo, mientras, en lo que respecta a los UAS de ataque, radica en que son sistemas de armas de un solo uso, ya que, aparte de los sensores, portan una cabeza de guerra, estando diseñados para destruirse en el ataque, al impactar contra su objetivo.

Las LM tienen diferentes alcances y autonomía de vuelo, pudiendo variar significativamente su forma, peso y la carga que transportan, incluyendo su cabeza de guerra. Si bien inicialmente su misión fue la de supresión de defensas aéreas enemigas (SEAD), hoy pueden llevar a cabo un gran número de misiones, pudiendo actuar con otros tipos de misiles, LM, UAS y los tradicionales sistemas de fuego indirecto (cohetes y morteros) en ataques coordinados.

Como se ha podido observar en los conflictos de Libia, Nagorno Karabaj y ahora en Ucrania, la gran mayoría de las LM empleadas podrían encuadrarse dentro de la categoría de los sUAS, los que las hace muy difíciles de detectar y neutralizar por parte de los sistemas de defensa aérea basados en superficie (SBAD) tradicionales. Sin embargo, este tipo de munición es susceptible de ser perturbada, al depender generalmente de sistemas de posicionamiento global (GNSS) y de enlace de datos para operar.

3. Entre lo necesario y lo posible: los sistemas C-sUAS

La vulnerabilidad de los UAS se ha puesto de manifiesto en aquellos conflictos en los que no han disfrutado de superioridad aérea o se han enfrentado a avanzados SDA, operados por personal bien adiestrado. Sin embargo, esto no ocurre con los sUAS, que operan en la capa más baja del espacio aéreo, fuera de la cobertura de las capacidades del SDA y también de los sensores de las agencias civiles de gestión de movimientos aéreos.

Las capacidades actuales del SDA no están diseñadas para detectar e identificar estos sistemas con una RCS muy reducida, que vuelan silenciosamente en la capa más baja del espacio aéreo, la más próxima a la superficie, a baja velocidad y con una firma infrarroja casi inexistente.

En este punto, es importante tener en cuenta que tampoco los sistemas SBAD existentes, al igual que sus sensores y efectores asociados, pueden

reconfigurarse para enfrentarse a esta nueva amenaza. Y esto también ocurre con las aeronaves de combate tripuladas, como es el caso de los cazas o los helicópteros. Estos sistemas son los que podemos denominar la generación 0 de los sistemas C-sUAS.

Esta situación empezó a cambiar con la entrada en servicio de los primeros sistemas específicamente creados para combatir los sUAS, que, en líneas generales, se articulaban en tres componentes principales:

- Subsistema de detección, seguimiento e identificación
  Constituido por sensores activos (radar) o pasivos (detección RF), dispondrá además de sistemas EO/IR que posibiliten el seguimiento, la clasificación, identificación e intención del sUAS.
- Subsistema de Mando y Control (C2)
  Capaz de generar una *Low Altitude Local Picture* del objetivo a defender, basándose en la información recibida por los distintos sensores integrados en el sistema asegura el flujo de órdenes e información entre todos sus integrantes, así como con aquellas otras estructuras de mando y control con las que se relaciona. A través de los elementos de detección, seguimiento e identificación, debe controlar el subsistema de interceptación/neutralización que se determine para cada situación.
- Subsistema de Interceptación/Neutralización
  Dependiendo del tipo de amenaza identificada, el análisis de la misión, las ROE en vigor, la valoración de riesgo y el estudio del posible daño colateral, se determinaría el efector a emplear, que puede ser actuar sobre la señal de control o de la señal GPS, tomar el control del sUAS, o incluso, la aplicación de soluciones cinéticas (en función de los sistemas de estas características disponibles y los posibles efectos colaterales que pudieran ocasionar).

Con carácter general, se considera a los sistemas C-sUAS como un «sistema de sistemas», cuyo funcionamiento se ajusta a diferentes fases en las que emplean distintas tecnologías:

- Prevención: En esta fase, las tecnologías estarán orientadas a obtener la inteligencia necesaria sobre los adversarios para poder enfrentar de forma más eficiente la posible amenaza. Para ello, se aplica el concepto de «atacar la red» de la doctrina C-IED, buscando identificar todos los actores (operadores, suministradores, fuentes de financiación, etc.) que permiten la operación de sUAS potencialmente hostiles, teniendo en cuenta que la explotación técnica de los mismos aportará información relevante en este proceso.
- Detección: Debe aspirarse a una combinación de sensores activos y pasivos, que permitan cubrir un amplio espectro (acústicos, radar, RF, etc.). La

combinación de ellos dependerá de su escenario de actuación, siendo más compleja en entornos urbanos y en aquellos donde puede haber interferencias en las frecuencias de operación (entornos aeronáuticos) e interferencias físicas que impiden la libertad de movimiento a la hora de operar.

- Identificación: Una vez detectado, se debe discernir entre amigo, enemigo o desconocido de forma rápida (acceso a librerías o sensores EO/IR).
- Decisión: Recibida la información de los sensores, el subsistema de mando y control es la herramienta principal para actuar contra la amenaza. La rapidez en la toma de decisiones se verá afectada por el grado de automatismo y la intervención del ser humano, que siempre deberá estar en la cadena de la decisión.
- Neutralización: En la fase final de la defensa C-UAS LSS, el objetivo es perturbar, controlar o destruir la amenaza, mediante el empleo de sistemas de armas cinéticas y no cinéticas.

Estos sistemas de 1.ª generación presentan ciertas limitaciones técnicas que afectan a las prestaciones proporcionadas por cada uno de sus subsistemas (Dominicus, 2021), viéndose condicionado igualmente su empleo por otras restricciones de carácter operativo y legal (DSN, 2022). Entre ellas, podemos citar:

- En lo que respecta a la detección, la configuración de la mayoría de estos sistemas solo contempla, generalmente, un único sensor. La tecnología más utilizada es la detección de señales de RF, en especial aquellas empleadas para el enlace de datos para controlar la aeronave, así como para transmitir la información obtenida por los sensores embarcados a la estación terrestre, lo que también pueden posibilitar la localización del piloto.
- La capacidad de detección de este tipo de sensores pasivos se puede ver limitada, en ocasiones de forma crítica, por aquellos sUAS que no emiten ninguna señal durante el vuelo, operando de forma autónoma o utilizando la tecnología 5G, o incluso, tras modificar sus enlaces de datos, de forma que las señales de estos sUAS no pueden distinguirse con respecto a otras análogas. Estos sistemas también contribuyen a la clasificación/identificación de cualquier sUAS que se encuentre dentro de su área de responsabilidad, cuando las señales que emiten son reconocidas dentro de las contenidas en su librería.
- Los siguientes sensores más empleados son los radares que, con respecto a este tipo de blancos, presentan limitaciones en cuanto a su alcance de detección, al desarrollar los sUAS perfiles de vuelo a muy baja altura y bajas velocidades, donde se pueden enmascarar con el terreno,

edificios, árboles, etc., aunque, por el contrario, si pueden detectar sUAS que operan de manera autónoma. En ocasiones, esos radares se combinan con sensores de detección de RF, operando asociados además a sensores EO/IR, les permite eliminar falsos positivos (por ejemplo, pájaros) y, sobre todo, completar el proceso de identificación de un posible sUAS potencialmente hostil.

- En todo el proceso de toma de decisiones, estos sistemas confían en la participación activa del operador en todas sus fases (*Human in the loop*), quien tampoco cuenta con herramientas que faciliten su labor, teniendo en cuenta que se trata de un proceso muy complejo y demandante, con numerosas funciones a realizar en poco tiempo y muchas variables a considerar (ROE, elección del efector, posibles daños colaterales, etc.).
- Al ser su conectividad muy reducida y no tener naturaleza modular, estos sistemas no son interoperables y no pueden integrarse con otros sistemas de C2 de otros fabricantes. Del mismo modo, su configuración no es modificable, no pudiendo incorporar más sensores o efectores.
- De forma similar a lo que ocurre con los sensores, en líneas generales, estos sistemas solo disponen de un tipo de efectores, principalmente no cinéticos (*jamming* y *spoofing* del enlace de datos-señal GNSS).
- Por último, es importante resaltar que estos sistemas pueden ser fácilmente superados y saturados por ataques de varios sUAS de manera simultánea.

La nueva generación de sistemas C-sUAS aporta mejoras significativas en lo que respecta a sus prestaciones, pero sobre todo también apuesta por introducir cambios en su filosofía de empleo, al apostar por aumentar su grado de autonomía, reduciendo el papel del operador en el ciclo de la decisión de los sistemas, de forma que pasemos de un sistema semiautónomo (*Human in the loop*) hacia un sistema supervisado (*Human on the loop*)[4].

La capacidad de detección de estos sistemas de 2.ª generación se basará en el empleo combinado de sensores de diferentes tecnologías, entre los que destacarán nuevos tipos de radares y donde seguirán estando presente detectores de RF, actualizados para actuar sobre enlaces de datos

[4] De acuerdo con la Directiva 3000/09 del Departamento de Defensa de los EE. UU. (noviembre de 2012), un sistema de armas autónomo es un sistema de armas que, una vez activado, puede seleccionar y atacar objetivos sin intervención posterior de un operador humano, mientras que los semiautónomos, tras su activación, solo actuarían contra un objetivo que haya sido seleccionado por un operador humano. Los sistemas supervisados serían aquellos que requieren la intervención humana para finalizar el cumplimiento de la misión.

modificados, cubriendo así todo el espectro de la amenaza. Seguirán contando con los sensores EO/IR o incluso LiDAR[5], además de disponer de *software* de reconocimiento de imágenes, que se verán potenciadas por la aplicación del *Machine Learning*[6].

El proceso de toma de decisiones también sufrirá modificaciones importantes, al poder disponer de una única COP (*Common Operational Picture*), resultante de la fusión de la información procedente de sus sensores, así como de un *software* de mando y control que permitirá la automatización de sus funciones. Entre estas, este *software* deberá llevar a cabo el proceso de evaluación y priorización de las amenazas tras ser identificadas, así como la selección y asignación del efector recomendado para actuar sobre cada una de ellas, lo que hará posible que puedan enfrentarse a ataques múltiples de sUAS.

En lo que respecta a los efectores a integrar, podrían contar con diferentes tipos, entre los que también se encontrarían del tipo cinético, incluyendo armas de energía dirigida, como los sistemas láser o microondas de alta potencia (HPM), e incluso sUAS del tipo *hunter-killer*, cuya misión es acometer y derribar sUAS hostiles[7].

En cualquier caso, hay que tener presente que, el muy superior ritmo en la evolución tecnológica de los sUAS sobre la de los sistemas diseñados para combatirlos hace que estos últimos tengan una clara posición de desventaja en su particular «juego del gato y el ratón», de forma que no solo nos obligará a convivir con esta amenaza, sino que además vamos a tener que asumir que la probabilidad de que pueda materializarse con éxito sea elevada (Chulilla Cano, 2023).

4. Mirando al pasado para afrontar los nuevos retos

Una vez identificada esta nueva amenaza, es necesario desarrollar e implementar por parte de nuestras FAS una capacidad integral C-sUAS que sea capaz de neutralizarla en sus posibles escenarios de actuación. Una capacidad que no se limita exclusivamente al desarrollo de sistemas C-sUAS, sino que, en línea con lo establecido por OTAN, se apoya principalmente en el empleo combinado de las capacidades de Defensa Aérea y de Protección de la Fuerza (CCDC EMAD, 2019).

5 LIDAR-*Laser Detection and Ranging*.

6 El reconocimiento de imágenes es un proceso ejecutado por un *software* de inteligencia artificial capaz de reconocer imágenes utilizando algoritmos matemáticos complejos. El reconocimiento de imágenes se apoya también en el *Machine Learning* y el *Deep Learning*.

7 El sistema LIDS del *US Army* ya emplea este tipo de sUAS, denominado Coyote.

En el desarrollo de esta capacidad adquiere una gran importancia el entorno en el que las operaciones se desarrollan, dentro o fuera de nuestras fronteras, así como si estas tienen lugar en tiempo de paz, crisis o conflicto armado. En Territorio Nacional (TN) y en tiempo de paz, la defensa C-sUAS recae de forma habitual en las Fuerzas y Cuerpos de Seguridad, si bien corresponde a las FAS como parte de la autodefensa de sus bases e instalaciones militares, lo que significa que, en ocasiones, las responsabilidades se pueden solapar, sobre todo en las zonas próximas a las mismas, por lo que es necesario delimitarlas con claridad y potenciar la coordinación y colaboración entre ambas fuerzas.

Con carácter general, hay que considerar que, enfrentarse a una nueva amenaza no se basa exclusivamente en crear y poner en marcha nuevas contramedidas específicamente diseñadas para ello. Esto es plenamente vigente en lo que respecta a la capacidad C-sUAS, cuya aplicación efectiva no descansa exclusivamente en la operación de sistemas C-sUAS diseñados para combatirla, sino en su empleo combinado con otras medidas de Protección de la Fuerza, muchas de ellas ya probadas de forma satisfactoria para oponerse a otras amenazas en el pasado, que nos permitirán hacerle frente con garantías y mitigar sus posibles efectos.

Estas medidas se extienden por todas las áreas de actividad en las que se agrupan las capacidades que proporcionan la Protección de la Fuerza tradicional, en especial dentro de las áreas de defensa activa y defensa pasiva[8]. En especial, es importante destacar su carácter preventivo, buscando negar la libertad y capacidad de acción a un posible adversario, con el fin de evitar que un acto hostil pueda producirse, o que, en caso de que sea así, minimizar sus consecuencias.

Contemplada en la doctrina OTAN, dentro de la defensa activa podemos citar el dominio de la zona que rodea a cualquier instalación, el Área Táctica de Responsabilidad (TAOR), que desempeña un papel fundamental para establecer una defensa efectiva de la misma. La TAOR debe extenderse más allá del perímetro de la instalación, con el fin de evitar que se puedan producir desde su exterior ataques directos e indirectos de tipo *stand off* contra la instalación, su personal y cualquier activo que opere desde la misma (ya sean aeronaves, buques o fuerzas terrestres).

[8] La defensa activa comprende el conjunto de actividades que permiten disuadir, detectar, prevenir o neutralizar las acciones del adversario que, llevadas a cabo en o desde el exterior de las instalaciones, persiguen influir, directa o indirectamente, en el desarrollo de las actividades de una Unidad. La defensa pasiva busca minimizar y mitigar los efectos de este tipo de acciones sobre la Fuerza, para aumentar su grado de supervivencia.

El dominio de esta TAOR, mediante una adecuada defensa terrestre y control de puntos clave (por ejemplo: cruces de carreteras) o dominantes (p. ej.: cotas o edificaciones singulares) ha sido totalmente necesario para el desarrollo de las operaciones C-RAM[9], C-IED y C-SAFIRE[10] en objetivos diversos, principalmente en bases aéreas, situados en Afganistán o Irak, entre otras zonas de operaciones. En el caso de las operaciones C-sUAS, es importante subrayar que para conseguir ese dominio de la TAOR también se emplearán sUAS propios en misiones de FP ISR y de corrección de tiro y munición merodeadora, sin descartar, en un futuro próximo, el uso de enjambres de sUAS. Esta medida sería de gran utilidad al objeto de evitar una posible acción hostil de sUAS que opera de manera remota en condiciones LOS, al limitar considerablemente, incluso denegar, la libertad de acción su piloto (o de los que pudieran intervenir en caso de un ataque combinado) para aproximarse a una distancia del objetivo que le permita llevar a cabo una acción hostil de estas características.

En Territorio Nacional, este tipo de medida es difícil de implementar en tiempo de paz. El marco legal existente en esta situación limita la capacidad de respuesta de las FAS a acciones contra sus bases e instalaciones militares, tanto en términos de ámbito de responsabilidad como de restricciones en el uso de la fuerza y sus posibles daños colaterales, correspondiendo la responsabilidad de llevar a cabo actuaciones similares fuera de la base o instalaciones militares a las FCSE, con independencia del tipo de instalación considerada. En el caso de las operaciones militares, su ejecución requerirá una estrecha y permanente cooperación entre de las FCSE y las FAS, en la que las actividades de adiestramiento conjunto para conocer las capacidades, tácticas, técnicas y procedimientos (TTP) de cada uno favorecerán la coordinación de sus actuaciones.

Otras medidas a considerar en este pilar son las tradicionales medidas de la defensa pasiva. Si bien gracias a las imágenes proporcionadas por los cada vez más avanzados sensores y satélites de observación, la presencia de dispositivos móviles, o el uso de internet, nos hace encontrarnos más expuestos y observados, y parece utópico pensar que un posible objetivo potencial pueda permanecer oculto o no ser localizado hoy en día, las características de la carga explosiva que es capaz de transportar un sUAS pueden no ser suficientes para destruirlo si este cuenta con elementos de protección física (incluyendo pantallas y redes de diverso tipo), que impidan

[9] *Counter Rocket Artillery and Mortar* —también denominado *Counter Indirect Fire*—, comprende aquellas medidas dirigidas a evitar o reducir las acciones de fuego indirecto contra el objetivo a defender.

[10] *Counter-surface to air fire,* medidas dirigidas a impedir las acciones contra las aeronaves propias, empleando armamento diverso desde superficie (desde misiles portátiles a armas ligeras), en las proximidades de sus bases aéreas.

el impacto directo (Guitton, 2021). La aplicación de otras medidas, como la dispersión, el uso generalizado de redes miméticas mutiespectrales que ofrecen una adecuada capacidad de camuflaje frente a sistemas de vigilancia radar, térmicos u ópticos, o la decepción mediante señuelos de diferentes tipos también incrementarán las probabilidades de supervivencia ante este tipo de ataques.

El tiempo es un factor crítico en las operaciones C-sUAS, considerando que la ventana disponible para completar su ciclo de decisión (*kill chain*) puede ser cuestión de muy pocos segundos, desde que se procede a la detección del sUAS y su identificación como hostil hasta que se selecciona y asigna el posible efector a emplear, tras analizar posibles daños colaterales. Por ello, ante esta situación tan demandante, es fundamental la figura del operador y todo lo que puede afectar a su actuación en el proceso de toma de decisiones, como es el caso de lo relativo a su formación y adiestramiento, al igual que a las reglas de enfrentamiento (ROE).

Más allá de la tecnología, como ocurre con cualquier capacidad militar, la formación y el adiestramiento del personal, tanto a nivel individual como colectivo, es un factor determinante para asegurar su empleo efectivo. Se da la circunstancia además que, desde el final de la Guerra Fría, las operaciones se han caracterizado por la ausencia total de amenaza aérea o por disfrutar de un grado de superioridad aérea tal que hacía que esta fuera considerada irrelevante (Haider y Milke, 2021). Por ello, con carácter general, se recuperarán muchos de los conceptos básicos ya utilizados en el pasado por otras capacidades, principalmente en el área de Defensa Aérea y de Protección de la Fuerza, adaptados a este tipo de operaciones. En cualquier caso, no basta con conocer y comprender la amenaza planteada por los sUAS, sino que es preciso mantenerse al día sobre su posible evolución.

Las ROE son la única autorización existente para el uso de la fuerza, en tiempo de paz y en el transcurso de operaciones, definiendo las circunstancias, condiciones, grado y procedimientos para su aplicación, más allá de la legítima defensa. Teniendo en cuenta estas circunstancias, propias de tiempo de paz, así como la complejidad de las operaciones C-sUAS cuando estas se desarrollan en las proximidades de las instalaciones militares y de su zona próxima de operación, se hace preciso establecer unas reglas de juego claras que se recojan en la doctrina de actuación y que permitan que los operadores cuenten con la seguridad jurídica necesaria en el desempeño de sus cometidos.

En este aspecto, conviene recordar que los sistemas C-sUAS actuarán siguiendo el principio de control centralizado y ejecución descentralizada, conforme técnicamente sea viable su integración en el SDA. En este contexto,

dado que el criterio de autodefensa regirá su actuación, será necesario que exista un acto hostil o una intención hostil para emplear la fuerza.

Será de vital importancia definir con claridad que es «intención hostil» en un entorno tan complejo, situado en las proximidades de la instalación, en el que pueden convivir sUAS potencialmente hostiles con los propios (incluyendo en esta categoría a los sistemas operados por las FAS y las FCSE) o con los operados por otros usuarios autorizados. Disponiendo de tiempos de reacción muy reducidos para tomar decisiones y actuar, implicará la necesidad de establecer estos criterios con antelación suficiente para ser incluidos en las correspondientes TTP, así como asegurarse de que el personal que opera estos sistemas C-sUAS se encuentra capacitado y adiestrado para ejecutarlas.

Es necesario referirnos también a la problemática para integrar esta capacidad en el SDA en TN, teniendo en cuenta que en la actualidad no se dispone de un sistema que permita ejercer el control (mediante la vigilancia, detección, identificación y actuación, si fuera preciso) y la coordinación de la capa más baja del espacio aéreo, donde conviven sUAS de uso civil (de uso comercial y recreativo), junto a sistemas militares y de otros organismos e instituciones del Estado.

El concepto de Defensa Aérea por capas permite que podamos abordar este problema, aunque para ello, debemos establecer un nivel de ambición realista definiendo burbujas de especial interés alrededor de infraestructuras críticas, bases aéreas e instalaciones militares, aeropuertos, edificios de interés, etc., donde se desplegarían sistemas C-sUAS autónomos que actuarían con protocolos de ejecución descentralizada (Esteban Muñoz, 2022).

Esto implicará la necesaria armonización de las responsabilidades de otros Ministerios (Fomento, Interior) en esta materia, con la misión permanente de vigilancia, control y defensa del espacio aéreo, de la que el Ejército del Aire y del Espacio es responsable. Para ello, se requerirá un subsistema que complemente al SDA, denominado SUCCAUL[11] (DSN, 2022). De naturaleza colaborativa, dicho subsistema ha de ser capaz de integrar y fusionar los datos de los sistemas propios, así como los que reciba de las FCSE, inicialmente del Sistema Integrado Global contra Drones (SIGLO-CD) y de otras organizaciones que se determine (como es el caso del Programa DOMUS de ENAIRE), contribuyendo a mejorar el conocimiento de la situación aérea de la capa más baja a través de una única imagen aérea en ese entorno, e incluso, cuando técnicamente sea viable, llegar a proporcionar alerta temprana en tiempo real, aumentando así los mínimos tiempos de reacción disponibles.

[11] SUCCAUL, Subsistema de Vigilancia, Control y Coordinación Aérea en entorno UAS LSS.

5. Conclusiones

Los sistemas de aeronaves no tripuladas han desempeñado un papel relevante en los últimos conflictos, lo que ha motivado que su uso se haya generalizado entre un número cada vez mayor de naciones, grupos no estatales y organizaciones terroristas, que ahora disponen de unas capacidades inherentes al Poder Aéreo que antes solo estaban al alcance de un reducido grupo de potencias militares.

La expansión y evolución tecnológica de los sUAS, así como su posesión y posible uso en acciones hostiles por parte de actores estatales y no estatales y organizaciones terroristas, supone una amenaza real y creciente para la seguridad de nuestras Fuerzas Armadas, en particular, tanto en Territorio Nacional como en el exterior como para el resto de la sociedad en general.

Los sUAS se encuentran en un proceso de evaluación permanente para aumentar sus prestaciones y reducir sus vulnerabilidades, en el que la inteligencia artificial y la tecnología 5G desarrollan un papel fundamental.

Ante la incapacidad de los tradicionales sistemas de Defensa Aérea para enfrentarse a esta amenaza, se ha constatado la necesidad de disponer de una capacidad C-sUAS para su empleo tanto en el exterior como en TN, que se apoya en el empleo combinado de las capacidades de Protección de la Fuerza y Defensa Aérea.

La capacidad C-sUAS tiene un carácter integral y no se basa exclusivamente en la operación de sistemas C-sUAS, sino también en la aplicación de otras capacidades y medidas de Protección de la Fuerza, que ya se han empleado en el pasado con éxito, las cuales siguen siendo plenamente vigentes, así como en la necesidad de contar con personal formado y bien adiestrado.

Las operaciones C-sUAS en TN presentan un mayor número de limitaciones y restricciones que las desarrolladas en el exterior, requiriendo una estrecha y permanente coordinación y colaboración con las FCSE y con otros organismos con los que se comparten responsabilidades en sus correspondientes ámbitos de actuación, así como la adaptación del Sistema de Defensa Aérea para llevar a cabo la vigilancia, control y la coordinación de la capa más baja del espacio aéreo.

Las mejoras que los nuevos sistemas C-sUAS plantearán con respecto a los actualmente en servicio no se limitarán al empleo de nuevos y más avanzados sensores y efectores, sino que irán dirigidas principalmente a introducir cambios en su filosofía de empleo, al apostar por aumentar su grado de autonomía, reduciendo el papel del operador en el ciclo de la decisión de los sistemas.

6. Bibliografía

Antebi, L. (2022). *Has Artificial Intelligence Triumphed over Terrorism? Lessons learned from the IDF's use of advanced technology in Operation Guardian of the Walls.* Air Power and New Technologies, 3. Disponible en: https://www.inss.org.il/wp-content/uploads/2022/06/Has-Artificial-Intelligence-Triumphed-over-terrorism-Liran-Antebi-1.pdf

Bari Urcosta, R. (2020). The Revolution in Drone Warfare: The Lessons from the Idlib De-Escalation Zone. *JEMEAA The Air Force Journal of European, Middle Eastern, and African Affaires*. Disponible en: https://www.airuniversity.af.edu/JEMEAA/Display/Article/2329510/the-revolution-in-drone-warfare-the-lessons-from-the-idlib-de-escalation-zone/

Bode, I. y Watts, T. (2023). *Loitering Munitions and Unpredictability: Autonomy in Weapons Systems and Challenges to Human Control.* Odense, Center for War Studies. Disponible en: https://www.autonorms.eu/wp-content/uploads/2023/06/Loitering-Munitions-Unpredictability-WEB.pdf

Bowden, M. (2022). The Tiny and Nightmarishly Efficient Future of Drone Warfare. *The atlantic*. Disponible en: https://www.theatlantic.com/technology/archive/2022/11/russia-ukraine-war-drones-future-of-warfare/672241/

Boyle, M. J. (2020). *The Drone Age. How Drone Technology will change War and Peace*. New York, Oxford University Press.

Centro Conjunto de Desarrollo de Conceptos. Estado Mayor de la Defensa. (2019). *CONCEPTO NACIONAL C-UAS LSS*. Madrid, Ministerio de Defensa. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/01_CONCEPTO_NACIONAL_C-UAS_LSS_xPARA_WEBx.pdf

Chávez, K. y Sweed, O. (2020). Off the Shelf: The violent Nonstate Actor Drone Threat. *Air & Space Power Journal*. 34. Disponible en: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F_Chavez_Swed.pdf

Chulilla Cano, J. L. (2023). Presente y Futuro de los Drones Comerciales Letalizados. *Revista General de Marina*. Disponible en: https://armada.defensa.gob.es/archivo/rgm/2023/05/RGMMayo2023Parte05.pdf

Dominicus, J. W. (2021). New Generation of Counter UAS Systems to Defeat of Low Slow and Small (LSS) Air Threat. *NATO SCI-301 Research Task Group (RTG)-MSG-SET 183 Conference Paper.* Amsterdam, Royal NLR - Netherlands Aerospace Centre. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjq9ly-2nI6CAxUPUKQEHcemC-wQFnoECBEQAQ&url=https%3A%2F%2Fwww.

sto.nato.int%2Fpublications%2FSTO%2520Meeting%2520Proceedings%2FSTO-MP-MSG-SET-183%2F%24MP-MSG-SET-183-KN-2.pdf&usg=AOvVaw3oCMaWc-VNZ11RWu8HzvAC&opi=89978449

Departamento de Seguridad Nacional. (2022). *Drones y Seguridad Nacional: Un estudio multidimensional*. Disponible en: htpps://www.dsn.gob.es/es/documento/drones-seguridad-nacional-un-estudio-multidimensional

Esteban Muñoz, A. L. (2022). Counter UAS ISS en el Ejército del Aire. Integración de la capacidad C-UAS en la estructura de mando y control del Ejército del Aire. *Revista de Aeronáutica y Astronáutica*. 911, p. 294. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/a/raa_911.pdf

Guitton, M. J. (2021). Fighting the Locusts: Implementing Military Countermeasures Against Drones and Drone Swarms. *Scandinavian Journal of Military Studies*. 4, pp. 26-36. DOI: 10.31374/sjms.53

Haider, A. y Milke, R. (2021). Education and Training. En: Harrigian, J L. (coord.). *A Comprehensive Approach to Countering Unmanned Aircraft Systems*., pp. 269-281. Joint Air Power Competence Center. Disponible en: https://www.japcc.org/chapters/c-uas-education-and-training/

Kallenborn, Z., Ackerman, G. y Bleek, P. C. (2022). A Plague of Locusts? A Preliminary Assessment of the Threat of Multi-Drone Terrorism. En: *Terrorism and Political Violence*. DOI: 10.1080/09546553.2022.2061960

Mackenzie, P. y Kanellos, F. (2021). Cyberspace Operations. En: Harrigian, J. L. (coord.). *A Comprehensive Approach to Countering Unmanned Aircraft Systems*., pp. 183-207. Joint Air Power Competence Center. Disponible en: htpps://www.japcc.org/wp-content/upload/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf

Rassler, D. (2018). The Islamic State and Drones: Supply, Scale, and Future Threats. *Combating Terrorism Center at West Point*. 7. Disponible en: https://ctc.westpoint.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf

Rogers, J. (2021). Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Ages. En: Harrigian, J. L. (coord.). *A Comprehensive Approach to Countering Unmanned Aircraft Systems*., pp. 481-505. Joint Air Power Competence Center. Disponible en: htpps://www.japcc.org/wp-content/upload/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf

Rogers, J. (2022). The Third Drone Age: Visions Out to 2040. En: *The Ethics of Automated Warfare and Artificial Intelligence*. Disponible en: https://www.cigionline.org/articles/the-third-drone-age-visions-out-to-2040

Rogers, J. (2023). The Second Drone Age: defining war in the 2020s. *Defense & Security Analysis*. 39, pp. 256-259. DOI: 10.1080/14751798.2023.2178519

Thomas, A. (2022). Les drones sur le champ de bataille: quelles leçons tirer de leur emploi par les forces ukrainiennes? *Défense & Industries*. 16. Disponible en: https://www.frstrategie.org/sites/default/files/documents/publications/defense-et-industries/2022/3.pdf

Veilleux-Lepage, Y. y Archambault, E. (2022). *A Comparative Study of Non-State Violent Drone use in the Middle East*. International Centre for Counter-Terrorism-ICCT. DOI: 10.19165/2022.3.01

Watling, J. y Waters, N. (2019). Achieving Lethal Effects by Small Unmanned Aerial Vehicles. *The RUSI journal*. 164, pp. 40-51. DOI: 10.1080/03071847.2019.1605017

Capítulo 2

Protección contra la Capacidad No Letal

Claudio Sánchez Sánchez

Resumen

Cada vez es más habitual que las fuerzas armadas y fuerzas y cuerpos de seguridad realicen operaciones en la llamada zona gris del espectro del conflicto, en la que se emplean sistemas no letales para evitar la escalada en el empleo de la violencia. En nuestro mundo globalizado cada vez es más fácil y más barato el acceso a cualquier tecnología. Estas son las dos principales razones para considerar como una seria amenaza para nuestras tropas el empleo de cualquier sistema no letal por parte de nuestros posibles adversarios.

Inicialmente, se definirá el concepto de arma/sistema no letal. A continuación, se detallarán los diferentes sistemas no letales en uso actualmente: los tradicionales empleados para control de masas, las armas láser, las de microondas (o de radiofrecuencia), las de haces de partículas, las armas sónicas e incluso las armas químicas y biológicas. Se explicará de forma sencilla en qué consisten cada una de ellas, sus ventajas, sus inconvenientes y sus posibilidades de empleo; detallando después las medidas pasivas y activas de protección que deberán tomar nuestros soldados, policías y guardias civiles para evitar sus efectos.

Palabras clave

Zona Gris, No Letal, Control de Masas, Armas de Energía Dirigida, Armas Láser, Microondas de Alta Potencia, Haces de Partículas, Armas Sónicas.

Protection against Non-Lethal Capacity

Abstract

It is increasingly common for armed and security forces to conduct operations in the so-called grey zone of the conflict spectrum, where non-lethal systems are used be employed to avoid escalation in the use of violence. Access to any technology is becoming easier and cheaper in our globalized world. These are the two main reasons for considering the use of any non-lethal system by our potential adversaries as a serious threat to our troops.

First, the concept of a non-lethal weapon/system will be defined. Second, the different non-lethal systems in use today will be detailed: traditional mass control weapons, laser weapons, microwave (or radio frequency) weapons, particle beam weapons, acoustic devices, and even chemical and biological weapons. To conclude, it will be explained in a simple way what each one of them consists of, its advantages, disadvantages and its possibilities of employment; later detailing the passive and active protection measures that our soldiers, police officers and civil guards must take to avoid its effects.

Keywords

Grey Zone, Non-Lethal, Crow and Riot Control, Directed Energy Weapons, Laser Weapons, High Power Microwave, Particle Beams, Acoustic Device.

1. Introducción

Recientemente, se está dando un gran impulso, en todas las Fuerzas Armadas (FAS) y Fuerzas y Cuerpos de Seguridad (FCS) del mundo, al desarrollo de una auténtica e integral capacidad no letal (CNL). Esta CNL permite neutralizar la amenaza de actividades de baja intensidad, evitando, en lo posible, el uso de la fuerza letal, cuando dichas actividades implican una amenaza para el cumplimiento de la misión propia, contra unidades desplegadas en operaciones e instalaciones militares, tanto dentro como fuera del territorio nacional.

La CNL es una necesidad esencial para poder cumplir las misiones en la denominada zona gris del espectro del conflicto, entre sus dos extremos: la guerra y la paz. Es fundamental dejar claro que esta CNL no sustituye, sino que complementa, a las capacidades letales/convencionales de las FAS y FCS de todos los países, e incluso de los grupos paramilitares, terroristas o de delincuencia organizada a los que se deba hacer frente[1].

Gracias al abaratamiento, a la facilidad de acceso a cualquier tecnología y a que numerosas empresas de seguridad y defensa de todo el mundo están desarrollando nuevas tecnologías que encajan en el concepto de capacidad no letal, cada vez será más probable que las unidades e instalaciones de las FAS españolas puedan ser atacadas (por cualquiera de las amenazas citadas en el párrafo anterior) con algún sistema no letal. Dichos actores hostiles se mueven perfectamente en la zona gris del conflicto y evitan las situaciones que permiten a las unidades propias el uso de la fuerza letal, aprovechando que nuestras unidades militares y policiales cumplan y respeten el Derecho Internacional Humanitario y la legislación nacional.

En este capítulo se pretende describir de una forma sencilla todos los posibles sistemas no letales que pueden ser empleados por nuestros potenciales adversarios, para enumerar después las medidas de protección (tanto pasivas como activas) que deben ser tomadas por nuestro personal para asegurar la Protección de la Fuerza en cualquier operación.

Se debe comenzar dando una definición de lo que se entiende por capacidad no letal. Aunque países aliados e incluso la OTAN dan otras definiciones, para este capítulo se tomará la empleada por el Ejército de Tierra (ET) español (Jefatura de Adiestramiento y Doctrina de Infantería, 2010):

> «Arma no letal es aquella que está específicamente diseñada y preparada para ser empleada con la finalidad de incapacitar al personal o material, minimizando las probabilidades de que

[1] Paradójicamente, la tecnología aplicable a la capacidad no letal no ha sido incluida en el proyecto n.º 2 PTP 2022-2024 *Tecnologías emergentes y disruptivas (EDT) de mayor interés/aplicación a nivel nacional*, del Centro Conjunto de Desarrollo de Conceptos del Estado Mayor de la Defensa, de mayo de 2023. En la próxima actualización de dicho documento deberá ser incluida.

> se produzcan muertes, daños a las propiedades y el medioambiente, buscándose, en lo posible, la reversibilidad de sus efectos. Incluye al armamento convencional empleado con los mismos propósitos mediante el uso de municiones, técnicas o accesorios apropiados».

De este modo, toda capacidad no letal, para ser considerada como tal y ser eficaz, debe cumplir los siguientes principios:

- Disuadir para lo que debe ser eficaz, tener alcance suficiente y poder integrarse fácil y rápido con el armamento letal.
- Provocar efectos que sean predecibles, graduables y potencialmente reversibles.
- Posibilitar la protección de las tropas propias ante sus efectos (tema central de este capítulo) y minimizar los daños colaterales.
- Poder operar en todo tiempo y ambiente.
- Posibilitar la creación rápida de obstáculos letales y no letales.
- Ser interoperables y modulares (personal, medios y procedimientos) para poder trabajar en un ambiente conjunto o combinado.
- Ser de fácil manejo.

Es fundamental establecer también desde el principio que pueden emplearse contra personal (individuos, grupos o masas), contra material (armamento, aparatos electrónicos o vehículos terrestres, aéreos y navales de todo tipo) y contra instalaciones/infraestructuras (comunicaciones, suministro de energía, agua, tráfico e infraestructura de transporte).

EFECTOS		GRADO	EJEMPLOS
Impide la actuación de personas o materiales	Incapacitación	Inconsciencia	Municiones contundentes
		Inmovilización total	Espumas adhesivas
			Dispositivos *taser*
		Destrucción de materiales	Microondas de alta potencia
			Pulso electromagnético
Elimina de forma efectiva la capacidad ofensiva del blanco sin incapacitarlo por completo	Neutralización	Sensorial	Láser
			Granadas aturdidoras
		Trauma	Proyectiles *foam*/goma
		Inmovilización parcial	Adhesivos de superficie
		Disrupción de funciones en materiales	Perturbadores
			Redes antimotrices

EFECTOS		GRADO	EJEMPLOS
La capacidad ofensiva o defensiva del objetivo permanecen, pero su motivación se ve afectada	Disuasión	Intimidación	Focos
			Municiones iluminantes
			Emisores acústicos
			Designación láser visible
		Huida de los efectos del arma	Energía dirigida
			Malodorantes
		Marcación e identificación	Munición de pintura

Tabla 1. Efectos y grados de los sistemas no letales, con posibles ejemplos[2].

2. Material de control de masas

De forma inmediata e inconsciente, al hablar de capacidad no letal, la mayoría de los lectores habrá pensado en el material de control de masas (o CRC *Crowd and Riot Control*), ya que es el más empleado por los ejércitos y fuerzas de seguridad y, por tanto, el que más se ha desarrollado en los últimos años. Además, es un material profusamente desarrollado en el sector civil de seguridad, fácil y barato de adquirir en cualquier país del mundo, por lo que será la amenaza más probable contra los miembros de nuestras FAS.

Los materiales CRC más comunes que pueden emplear nuestras tropas o cualquier tipo de adversario son:

- Porra/defensa, tanto extensible como rígida, de una longitud de 1 m.
- Espray con gas pimienta con un alcance de 4 a 8 m.
- Inmovilizadores musculares portátiles (conocidos coloquialmente como *taser*), las pistolas tienen un alcance máximo de 10 m. También los hay múltiples, para formar una barrera contra varios adversarios, como el *Taser Shockwave* que dispone de 36 disparadores en dos filas, tiene un alcance máximo de 12 m.
- *Modular Crowd Control Weapon* (MCCW): se trata de minas direccionales antipersonales (tipo *claymore*) dispersadoras de bolas de goma (unas seiscientas cada mina), con un alcance máximo de 15 m.
- Proyectiles de goma (caucho o espuma *foam*), o con munición marcadora para escopeta de 12 mm con un alcance de solo 10 a 50 m.

[2] Cuadro extraído del experimento MA22-05 sobre el concepto operativo de la capacidad no letal, desarrollado por el Regimiento de Infantería (RI) Palma n.º 47 del Ejército de Tierra, durante 2022 y 2023. Es importante resaltar que el RI Palma n.º 47 es la unidad de referencia del ET y por extensión de las FAS españolas, en la experimentación para implantar una auténtica capacidad no letal.

- Cañones de agua, el portátil tiene un alcance de 12 m, mientras que el instalado sobre vehículo alcanza los 40 m.
- Granadas de mano de diferentes tipos: dispersadoras de submuniciones de goma; de efecto *flash bang* (conocida como *Stun*)[3]. Todas tienen poco alcance, como máximo 40 m.
- Proyectiles para lanza granadas portátiles de 40 mm, los de goma tienen un alcance de solo 10 a 50 m, mientras que los lacrimógenos y los de efecto *flash bang* pueden alcanzar los 300 m.
- Granadas para los lanzadores de artificios que portan todos los vehículos de combate de 76 mm (aunque también los hay de 66 mm), las lacrimógenas con un alcance de 60 a 85 m, mientras que las de efecto *flash bang* pueden alcanzar los 150 m[4].
- Vehículos aéreos no tripulados (UAV) portadores de sistemas no letales: lanzador de bolas de goma, o un marcador (*marking powder*) para facilitar la posterior localización de individuos o vehículos.

Como se puede deducir fácilmente tras la lectura de los alcances máximos de estos materiales, la mejor medida pasiva de defensa (gratuita) frente a todas estas amenazas es mantener una distancia de seguridad, entre nuestros soldados y los eventuales agresores, de unos 20 m; para proteger los acuartelamientos e instalaciones bastará con aplicar el tradicional perímetro de seguridad. Para mejorar esta protección y extenderla a patrullas móviles es necesario adquirir redes tácticas antidisturbios, como la TACRION (*Tactical Riot Net*): es una valla portátil, ligera y muy resistente de 2,5 m de alto y 35 m de largo, para crear una barrera eficaz contra personal y prevenir o controlar disturbios; puede utilizarse con una cubierta contra la observación que evita la detección visual, el infrarrojo térmico, el infrarrojo cercano y el radar.

Otra medida pasiva, sencilla y de bajo coste, consiste en dotar a todos nuestros soldados con protecciones individuales: uniforme especial antitraumas (un auténtico uniforme de combate, similar al que ya tienen en

[3] Las granadas *flash bang* reciben ese nombre al combinar dos efectos: el visual, ya que provocan un destello muy intenso (*flash*) que ciega y el sonoro (*bang*), al detonar de forma muy intensa que aturde; pero no producen ninguno de los efectos letales de las granadas: térmicos, onda de choque y dispersión de metralla.

[4] Por ejemplo, la granada de fabricación española Escudo AR (empresa Falken S. A) es una munición para los lanzadores de artificios de 76 mm que combina efectos de aturdimiento (por el sonido de la explosión), cinéticos (por la proyección de bolas de caucho) e irritante (gases lacrimógenos). Su finalidad es garantizar la supervivencia de un vehículo militar que se vea rodeado y potencialmente expuesto a agresiones con objetos contundentes o incendiarios, lanzados por una fuerza aparentemente hostil (habitualmente compuesta por personal civil), sin producir daños irreversibles sobre los agresores.

dotación algunos ejércitos de países de nuestro entorno), guantes de combate, chaleco antibalas, escudo, protecciones corporales y protección facial para el casco (estos tres últimos equipos pueden ser normales o con protección balística). Durante la instrucción se acostumbrará a todos los miembros de la unidad (militar o policial) a llevar permanentemente todo el equipo: uniforme completo con mangas bajadas, guantes, chaleco y casco; las protecciones corporales, la facial y el escudo estarán a mano (por ejemplo, en el vehículo de la patrulla), para poder incorporarlos rápido ante un aumento de la amenaza.

Para protegerse contra las granadas ensordecedoras (*flash bang*), que emiten un ruido generado por un explosivo para desorientar a determinados individuos, se debe generalizar el empleo de auriculares de última generación[5] que incorporan tanto la protección auditiva como la reducción activa de ruidos.

Cada soldado dispondrá de su máscara antigás reglamentaria (actualmente es la NBQ M6-87 con dos filtros) para prevenirse frente a las granadas lacrimógenas. Se debe insistir en que todo combatiente debe estar instruido para colocarse de manera correcta esta máscara en nueve segundos desde que se da la alarma y que cada filtro, en un ambiente de contaminación media, mantiene sus propiedades y eficacia durante una hora aproximadamente.

Para protegerse frente a agresiones realizadas por personal desarmado empleando vehículos de motor, se pueden adquirir diferentes sistemas:

- Dispositivo de desinflado de neumáticos (*spike strip*), para detener rápidamente vehículos terrestres mediante una tira de púas o pinchos metálicos. Pueden ser fijos para proteger instalaciones, o portátiles para pequeñas unidades militares o policiales.
- Red para la detención de vehículos (*x-net*), tiene la misma finalidad que la tira de clavos, pero es más segura para el conductor y el vehículo. Consiste en una red que se lanza o dispara contra las ruedas del vehículo, enrollándose en ellas y deteniéndolo en pocos metros.
- Barreras para detener vehículos terrestres en ataque de embestida, pueden ser las clásicas fijas de hormigón colocadas en las instalaciones permanentes, o barreras portátiles y modulares, como el modelo F-11 de Pitagone que es capaz de resistir el choque de un camión de 7,5 t a 48 km/h.

[5] Como el protector auditivo y de comunicaciones EMTM PELTORTM ComTacTM VI NIB que actualmente se están experimentando en el Programa de Sistema de Combatiente a Pie (SISCAP) español. Protectores similares incorpora el Land Capability Group Dismounted Soldier System (LCGDSS) de la OTAN y el nuevo programa de capacidad aumentada para el soldado futuro Achile de la Unión europea (UE).

Por último, las experiencias obtenidas de los últimos conflictos bélicos (especialmente en Nagorno Karabaj, en 2020, y en Ucrania, tanto en 2014-2015 como en 2022-2023) reflejan que todas las pequeñas unidades de nuestras FAS deberán incorporar sistemas contra UAV para garantizar su protección contra estos omnipresentes sistemas. A los efectos de defendernos contra esta amenaza, es indiferente que el UAV enemigo emplee sistemas letales o no letales contra las fuerzas propias, por lo que se puede adquirir un único sistema C/UAV con capacidad para detectarlo, seguirlo y neutralizarlo. El abanico de sistemas disponibles actualmente es muy amplio. Como principal medida pasiva se destaca el empleo de redes de enmascaramiento o cubiertas superiores que impidan la observación sobre las tropas propias y, en la seguridad de instalaciones, el empleo de las clásicas garitas que permitan la observación hacia el exterior y la impidan hacia el interior. Como medidas activas se destacan todos los sistemas portátiles en desarrollo: escopetas de intervención de 12 mm, ametralladoras de cualquier calibre, armas láser de alta energía, armas de energía dirigida, etc.

3. Armas de energía dirigida

Las armas de energía dirigida (DEW[6]) están diseñadas para dañar objetivos a largas distancias empleando energía concentrada, emiten energía en una dirección específica sin usar un proyectil. Transfieren energía a un objetivo para obtener un efecto deseado, pudiendo causar en los seres humanos efectos letales o no letales. Transportan la energía utilizada a través de ondas electromagnéticas o partículas atómicas o subatómicas. Se pueden identificar cuatro tipos fundamentales de DEW en función de sus características y efectos:

- Las armas láser[7], que utilizan la emisión inducida o estimulada de fotones para generar un haz de luz monocromática, coherente, espacial y temporalmente, en una dirección, concentrando gran cantidad de energía en un punto concreto.
- Las armas de microondas (o de radiofrecuencia), que emplean una emisión direccional de radiofrecuencia de alta energía, con frecuencias ubicadas en el rango de las microondas.
- Las armas de haces de partículas, que usan un haz de alta energía de partículas atómicas o subatómicas en una dirección determinada para dañar un objetivo, afectando su estructura atómica o molecular.

6 DEW, Directed Energy Weapons.

7 LASER, Light Amplification by Stimulated Emission of Radiation, amplificación de luz por emisión estimulada de radiación.

- Las armas sónicas, que se basan en la propagación direccional de ondas mecánicas generadas por el movimiento vibratorio de un cuerpo, sean audibles o no, a través del aire.

En el momento de considerar la integración de estas armas en las capacidades de las FAS españolas, o en las de nuestros potenciales adversarios, ya que este es el objeto de esta publicación, es necesario tener en cuenta sus ventajas y sus limitaciones.

Como ventajas comunes a todas las armas de energía dirigida se pueden señalar:

- Discreción. La radiación por debajo o por encima del espectro común no genera ningún tipo de sonido y no es visible para el ojo humano.
- Precisión. No se ven afectadas por la gravedad, viento o fuerza de Coriolis[8] debido a la ausencia de masa (no se dispara ningún proyectil) por lo que el proceso de puntería es más preciso.
- Velocidad y alcance[9]. Los láseres y microondas viajan a la velocidad de la luz, por lo que el objetivo se adquiere de manera instantánea y a un alcance teóricamente infinito.
- Gradualidad. Se pueden variar los efectos deseados dentro de un mismo sistema regulando su potencia o empleando varios sistemas DEW.
- Disminución de la carga logística. Desaparece prácticamente la necesidad de la reposición de munición, siempre y cuando se asegure el suministro de energía para estas armas.
- Economía. A pesar del elevado coste del sistema, el «disparo» o «proyectil» apenas supone gasto, por lo que, a medio plazo, puede resultar mucho más asequible que el armamento convencional.

Sus limitaciones son:

- Se pierde potencia de disparo si el haz se difracta y si elementos atmosféricos o los cambios de densidad del aire provocan su dispersión.
- Están condicionadas por la capacidad de obtención de energía, ya que su eficiencia en la actualidad oscila entre el 10 % y el 30 %.
- El tiempo de carga entre disparos puede ser de tres segundos o más.
- Su efectividad puede verse neutralizada por objetos que reflejen o inhiban los haces que envía el arma.
- En general ocupan un gran volumen debido al tamaño actual de sus generadores de energía.

[8] La fuerza de Coriolis es una fuerza ficticia que actúa sobre los objetos que se mueven en un sistema de referencia en rotación, como la Tierra. Esta provoca que los objetos desvíen su trayectoria, siguiendo una curva en lugar de una línea recta.

[9] Esta ventaja de las armas de energía dirigida no se aplica a las armas sónicas.

4. Armas láser

Los componentes genéricos de un láser son siempre los mismos: una fuente de alimentación con combustible, una cámara donde se genera luz coherente, la óptica para formar y enfocar un haz, los sensores para rastrear los objetivos y determinar la distancia entre el láser y, por último, los medios y técnicas de control de haz para que atraviese el espacio con máxima eficiencia.

Si se quiere emplear como arma, es necesario además dotar al conjunto con un sistema de puntería y control, basado en un radar, medios ópticos o ambos. Debe ser capaz de mantener el láser apuntado sobre el objetivo hasta producir los efectos buscados.

Los efectos del láser dependen de la potencia del arma, de las condiciones ambientales que pueden degradar el haz y de las medidas de protección de que disponga el blanco. Su letalidad está determinada por la interacción de su potencia, longitud de onda y sistema óptico. Por último, su efectividad depende también de las características del objetivo: es más fácil neutralizar la optrónica de un sistema de vigilancia estático que derribar un vehículo aéreo, debido a que el primero requiere menos potencia y capacidad de mantener fijado el objetivo que el segundo.

Desde el punto de vista de las aplicaciones militares, los láseres se pueden agrupar en dos grandes categorías atendiendo a la energía que generan: de baja y de alta energía.

Los de baja energía están desarrolladas como armas no letales, incapacitando al personal al producir pérdida de visión temporal cuando se apunta a los ojos del individuo o a los sensores del vehículo en el que se encuentra. Estas armas se conocen con el nombre genérico de *dazzler* (deslumbrante en inglés) y su finalidad es desactivar, cegar o desorientar temporalmente a su objetivo, sensores o personal, con una intensa radiación láser de baja energía mediante la emisión de una luz infrarroja cuando actúan contra los sensores electrónicos y luz visible contra los humanos. La mayoría de los sistemas son portátiles y funcionan en las áreas rojas o verdes del espectro electromagnético. En las personas, los efectos pueden ser la ceguera temporal en la visión causada por un destello, la incapacidad de ver causada por la luz brillante o la imagen que permanece después de exponerse a una luz brillante. Esta distracción, desorientación o malestar que se produce son incapacitantes para pilotos de avión, conductores y operadores de sistemas.

Algunos ejemplos de estas armas son: el deslumbrador láser portátil empleado por la Armada norteamericana BE Meyers Glare LA-9/P, con un alcance de 4 km por la noche y 1,5 km durante el día; el fusil chino PY132A

con un alcance de 400 m, puede realizar diez mil disparos y deslumbra al personal de diez a sesenta segundos.

Las armas de láser de alta energía son las que tienen una mayor aplicación en el campo de batalla actual, buscan la destrucción del objetivo, por lo que pueden ser utilizadas contra material o infraestructura. Hay tres tipos principales de láser de alta energía (HEL): láser químico, láser de estado sólido y láser de electrones libres. Más allá de las diferencias en los medios de generación, cada tipo tiene atributos fundamentales que afectan a su capacidad de madurar como armas operativas. Los láseres químicos son los únicos sistemas láser actuales capaces de alcanzar la potencia necesaria para interceptar objetivos como misiles balísticos a cientos de kilómetros. Los láseres de estado sólido fueron los primeros en ser desarrollados para diferentes usos (de baja energía para reproductores de DVD e impresoras láser y de alta energía para telémetros, radares, designadores de objetivos y sistemas de defensa de contramedidas). Los que se están desarrollando en los últimos años son los de clase kilovatio (HEL) pensados contra amenazas RAM (*Rockets, Artillery and Mortars*) y UAV LSS (*Low Slow and Small*, pequeños, que vuelan despacio, haciendo poco ruido y muy bajos, habría que añadir también baratos). Los láseres de electrones libres (FEL) tienen un gran interés debido a su potencial para lograr las altas salidas de potencia necesarias para interceptar misiles balísticos y su capacidad para «sintonizar» sus haces a diferentes longitudes de onda de manera que puedan progresar mejor en las atmósferas densas y húmedas de los entornos marítimos. Actualmente, los FEL aún son muy grandes e ineficientes, por lo que no son de utilidad para las FAS.

Las principales ventajas de las armas láser son: tienen un muy bajo costo por disparo en contrapartida con el coste de un proyectil guiado disparado por cañón; tienen un cargador casi ilimitado, pues pueden ser disparados indefinidamente mientras la plataforma disponga de combustible; sus tiempos de adquisición son muy cortos; su capacidad para contrarrestar misiles que efectúen maniobras drásticas; discreción de empleo al ser silenciosas; muy alta precisión y permiten realizar respuestas graduadas mediante la regulación de su potencia de salida.

Como limitaciones potenciales hay que señalar los siguientes factores: tanto la adquisición del objetivo como el ataque dependen de que haya visión directa; su precisión está influida por la absorción atmosférica, la dispersión y las turbulencias; el calor generado por el propio haz puede desenfocarlo; su sistema de puntería puede ser saturado mediante ataques simultáneos por el tiempo necesario para atacar cada objetivo y existe un elevado riesgo de daños colaterales por el alcance, en teoría ilimitado, del haz.

Para protegernos de sus efectos (peligro para los ojos, para la piel e incendios) deberemos tomar las siguientes medidas:

La medida pasiva más eficaz es el uso de filtros ópticos de banda estrecha sintonizados con la frecuencia del láser, ya sea mediante el uso de gafas apropiadas a la longitud de onda de cada láser; acoplando filtros de protección láser a las gafas de protección reglamentarias en las FAS, o integrándolos como viseras en los cascos reglamentarios (de combate, de tripulación de vehículo o de piloto de aeronave). Los filtros a base de polímeros son ligeros y económicos, protegen contra láser de baja potencia; los fabricados en vidrio proporcionan un mayor grado de protección contra láser de potencia moderada y alta. Para contrarrestar esta sencilla (y barata) defensa, la mayoría de los deslumbrantes (*dazzler)* actuales emplean emisores con varias longitudes de onda o láser sintonizables con un rango de salida más amplio. Otra medida es el empleo de gafas de protección de material fotocromático, capaces de volverse opacas bajo altas densidades de energía luminosa. También se están investigando técnicas de óptica no lineal: por ejemplo, ya es posible el empleo de limitadores ópticos de teluro de zinc dopado con vanadio (ZnTe:V) ligeros y compactos, capaces de bloquear un haz deslumbrante de alta intensidad, mientras deja pasar la imagen de menor intensidad[10].

El uniforme de combate debe tener cierto grado de protección contra la radiación láser directa o difusa. Como ya se ha dicho antes, se debe diseñar y empezar a emplear en las FAS españolas un auténtico uniforme de combate con prestaciones mucho mejores que nuestro actual uniforme de campaña, que en realidad debe ser considerado solo como un uniforme de trabajo o de instrucción; de forma muy similar a lo aplicado por la Unidad Militar de Emergencias (UME), que emplea como uniforme de trabajo diario su conocido uniforme negro, pero para cada riesgo emplea un uniforme de intervención específico (incendio, inundaciones, incidente NBQ, etc.)[11].

En las instalaciones fijas se pueden instalar filtros en las ventanas de las garitas del personal de seguridad, la forma más sencilla es colocando películas (*film*) adhesivas de protección láser.

También se dispone de pantallas portátiles de seguridad, aunque de momento son pequeñas (uniendo paneles de 2 m de alto y 1,80 m de ancho).

Otra medida pasiva es el empleo de alertadores de iluminación láser, su instalación en los vehículos militares es muy sencilla y en la actualidad se estan

[10] Los requerimientos que se exigen a estos sistemas de protección ocular están detallados en el NATO *Standard* AEP-4495 *Guidance for the procurement of laser eye protection* (LEP) *for the individual military user*. Edition A Version 1 (septiembre de 2016) y en el NATO *Standard* AAMedP-1.14 *Minimum requirements for aircrew protection against the hazards of laser systems and devices.* Edition B Version 1 (septiembre de 2022*).*

[11] El Reglamento (UE) 2016/425 del Parlamento Europeo y del Consejo de 9 de marzo de 2016, relativo a los equipos de protección individual contra láser, no se aplica de forma obligatoria a los componentes de las FAS y FCS, pero sería conveniente ir aplicando alguno de sus requerimientos al futuro uniforme de combate.

desarrollando versiones muy ligeras para integrarlas en el casco y chaleco de los soldados a pie (de momento solo en unidades de operaciones especiales). Estos sistemas emiten una señal acústica o luminosa cuando el objetivo (vehículo o persona) es iluminado por un haz láser. Algunos modelos incluso dan coordenadas polares del láser que nos ilumina. Facilitando no solo ocultarse de su haz, sino también cualquier reacción ofensiva contra el emisor.

Como medida activa no letal ya se están desarrollando botes fumígenos de ocultación anti láser, en calibre 40 mm, para ser lanzados desde el lanzagranadas acoplado al FUSA HK G-36 de las FAS españolas, así como en calibre 76 mm para ser disparados desde los tubos lanza artificios de los vehículos de combate.

Como el fuego es el tercer riesgo asociado al empleo de láser de alta potencia, se deberán tomar las medidas habituales para la extinción de incendios en vehículos e instalaciones.

5. Armas de microondas

Las armas de radiofrecuencia, también conocidas como armas de microondas, son aquellas que emplean la parte del espectro electromagnético usada en las transmisiones de radio; incluyen las bandas UHF (300 MHz-3 GHz), SHF (3-30 GHz) y EHF (30-300 GHz). Incluyen a las armas de microondas de alta potencia (HPM), que se subcategorizan como sistemas de banda estrecha (NB) o banda ultra ancha (UWB). Estas HPM son sobre las que se centran la mayoría de las investigaciones y desarrollos, presentando cada uno de estos tipos ventajas e inconvenientes: las de NB producen más potencia, tienen mejores características de transmisión y menos posibilidad de afectar a los sistemas amigos, pero son más susceptibles a contramedidas; mientras que las que emplean UWB aplican menos energía, pero proporcionan un amplio abanico de capacidades, por lo que afectan a una multitud de sistemas diferentes, pero su alcance eficaz es más corto que las de banda estrecha por su menor potencia de emisión.

Existen dos clases principales de armas de radiofrecuencia, cuyas diferencias vienen definidas por su modo de emisión, por su potencia, su carácter y su finalidad:

- Unas son las que se basan en el Pulso Electromagnético (EMP, *Electromagnetic Pulse*). Emiten pulsos de muy alta potencia, suelen ser ofensivas y se emplean contra el material, actuando por estimulación eléctrica. Al llegar las microondas a los componentes electrónicos del objetivo, se produce una estimulación eléctrica que transmite la energía a los componentes electrónicos a través de los circuitos del propio objetivo; el tiempo requerido para alcanzar los efectos es muy breve, por lo que tienen una gran eficacia.

- Las segundas emiten una onda continua de alta potencia, son principalmente defensivas y se empleadas básicamente contra personal, causando sus efectos por calentamiento molecular. La potencia requerida para obtener este efecto en las moléculas es bastante grande y necesita un tiempo de actuación significativo del haz sobre el objetivo deseado[12].

Las capacidades que aportan este tipo de armas son: economía, por su bajo coste de funcionamiento; mínima carga logística; rapidez de puesta en funcionamiento; idéntico empleo diurno y nocturno; posibilidad de empleo en entornos urbanos y efectos contra múltiples objetivos de manera simultánea y con diferentes efectos.

Como limitaciones principales se pueden señalar: su alcance efectivo es inferior a las armas cinéticas (las de EMP contra materiales alcanzan unos 1.000 m, mientras que las empleadas contra personal solo alcanzan unos 100 m); la potencia del haz disminuye sensiblemente con los accidentes atmosféricos: humedad, niebla, polvo, etc.; son detenidos fácilmente empleando barreras físicas de todo tipo (por ejemplo la puerta transparente de nuestro microondas de la cocina); tienen un elevado riesgo de dañar elementos propios y emiten una firma electrónica sencilla de localizar.

A finales de 2016, en el incidente conocido como síndrome de La Habana, veintiún funcionarios de la embajada norteamericana de la capital cubana (tanto marines en función de seguridad exterior como diplomáticos y sus familiares), escucharon ruidos extraños, sufrieron fuertes dolores de cabeza, náuseas y problemas con el equilibrio o el vértigo; incapacitando temporalmente a algunos de ellos. En un principio se pensó que habían sufrido un ataque con armas sónicas, pero tras las minuciosas pruebas realizadas, los expertos se inclinan más por un ataque con armas de microondas. Los norteamericanos habrían sufrido el efecto auditivo de microondas (AEM), también conocido como «efecto Frey», que provoca mareos, dolores de cabeza y sensación de hormigueo cuando se somete a los sujetos a una radiación por microondas adecuadamente pulsada a una distancia máxima de 100 m desde el transmisor. Los rápidos pulsos de microondas calientan ligeramente los tejidos blandos del cerebro, provocando una onda de choque dentro del cráneo.

En 2004 los EE. UU. desarrollaron el sistema MEDUSA (Mob Excess Deterrent Using Silent Audio) basado en este principio y se tiene la certeza de que tanto China como Rusia poseen sistemas similares.

[12] Por ejemplo, el sistema norteamericano Active Denial System (ADS) emite un haz microondas de alta frecuencia contra personas, con una longitud de onda de un milímetro o inferior, las ondas penetran en la piel unos 0,4 mm e inducen un calentamiento del agua subcutánea que provoca una sensación de quemadura. En dos segundos se alcanza una sensación térmica de 54.º C y el cuerpo reacciona por acto reflejo al llegar a los 50º C apartándose, pudiéndose aguantar solo unos cinco segundos.

Para protegernos de sus efectos deberemos tomar las siguientes medidas:

La única defensa pasiva efectiva contra el EMP es el aislamiento eléctrico completo, consistente en una jaula de Faraday, estructura metálica que distribuye la radiación recibida por todo su exterior, impidiendo su acceso al interior; como efecto adverso, puede restringir la transmisión y recepción de frecuencia modulada (FM). La mayoría de los equipos militares la tienen, pero no los equipos civiles. Actualmente, estan disponibles en el mercado telas especiales Faraday fabricadas con fibras metálicas finas para aislar y proteger en su totalidad los equipos sensibles (móviles, ordenadores portátiles, GPS, etc.).

Para los empleados contra las personas, la principal es (de nuevo) mantener una distancia de seguridad sobre el posible emisor, puesto que sus alcances son de 80-100 m; así como el empleo del uniforme de combate completo con guantes, casco y protecciones oculares y acústicas, ya que mitigan el efecto calórico sobre el cuerpo humano. Al igual que se ha dicho, al tratar la protección contra los láseres, sería conveniente que los nuevos uniformes de combate contasen en su tejido con protección contra la radiación de microondas (ya esta disponible en el mercado y no es cara), e incorporasen una capucha (como los uniformes NBQ) para protegerse del efecto auditivo de microondas (sufrido en el síndrome de La Habana). Para proteger el material bastaría con añadir en las ventanas/parabrisas protecciones transparentes tipo cortina o autoadhesivas.

Como medidas activas, la más sencilla y eficaz es el movimiento, para tratar de salir del haz del pulso de microondas. También localizar con medios electrónicos propios el transmisor de microondas y neutralizarlo empleando cualquier medio propio no letal (para no provocar una escalada en la aplicación de la violencia).

6. Armas de haces de partículas

El fundamento teórico de este tipo de armas se basa en acelerar partículas atómicas o subatómicas y formar con ellas un haz que viaje a velocidades cercanas a la luz, de manera que al impactar transmitan su energía cinética al blanco. Sus efectos pueden ser: aumentar la temperatura del blanco, penetrar su superficie, provocar una explosión o causar daños por la radiación. En teoría, pueden alcanzar una potencia muy superior al resto de armas de energía dirigida, aunque a costa de una mayor demanda energética y tamaño, lo que dificulta su desarrollo y despliegue sobre el terreno. Existen diversos tipos de armas: las de haces de partículas propiamente dichas, por ahora armas están todavía en fase de investigación y es probable que pase mucho tiempo antes de ver sus aplicaciones prácticas como armas; y las de plasma, de las que tampoco hay por el momento desarrollos

de armas basadas solo en este principio. Por tanto, no se considerarán en este capítulo.

Otros sistemas que podrían encuadrarse dentro de las armas de partículas son diversos tipos de cañones de agua, en las que las partículas empleadas son las propias moléculas de agua a las que se inducen ciertas propiedades, especialmente conductividad eléctrica, para obtener determinados efectos. Existen diversas propuestas de cañones que emplean agua electrificada para conseguir los efectos de electrochoque tipo *taser* cuando se necesita controlar a más de una persona. De momento ningún sistema ha pasado de la fase de proyecto. Como ya se citó al hablar de ellos dentro de los sistemas de control de masas, sus dos grandes inconvenientes son su corto alcance (unos 12 m los portátiles y 40 m los instalados sobre vehículos) y un número de «disparos» limitado por la capacidad del depósito.

Las medidas de protección contra ellos son muy sencillas: mantener una distancia de seguridad proporcional al tipo de cañón empleado, interponer una barrera física de suficiente consistencia para evitar sufrir el impacto directo del chorro de agua y esperar a que consuma el agua del depósito[13].

7. Armas sónicas

El oído humano puede captar las frecuencias comprendidas entre 20 Hz y 20 kHz. Las frecuencias que se encuentran por debajo de este rango se denominan infrasonidos (menos de 20 Hz) y las que se encuentran por encima ultrasonidos (a partir de 20 kHz). Las ondas sonoras pueden tener efectos tanto físicos como psicológicos, desde presión y dolor en el oído interno, hasta dificultad para respirar con sonidos de una intensidad de 66 dB. Los sonidos de bajas frecuencias tienen la capacidad de provocar estados de ansiedad, vértigos, náuseas y cefaleas, mientras que en el otro lado del espectro las frecuencias de los ultrasonidos producen cavitación en los líquidos, o formación de burbujas, al igual que un aumento de temperatura en las partes del cuerpo afectadas.

Uno de los principales problemas de las ondas sónicas para su empleo como arma es su emisión en forma de propagación omnidireccional, ya que es difícil concentrar sus efectos en una dirección concreta. En general, los sonidos de altas frecuencias son más direccionales, pero se atenúan antes (por lo que su alcance es menor), mientras que los de baja frecuencia tienen mayor rango de acción, pero menos direccionalidad. Su gran ventaja es que se propagan sin problemas en condiciones atmosféricas adversas

[13] Por ejemplo, el Wasserwerfersystem Feldjäger del Ejército alemán tiene un peso de 13 t y un depósito de agua con 920 l de capacidad. En cada disparo se consumen 12 l (individual) o 24 l (doble), por lo que el número máximo de disparos que puede hacer es de 38 a 75.

como lluvia, humo, polvo, etc. Por la forma de transmitir la energía, las armas de ultrasonidos son mucho más efectivas bajo el agua que en el aire.

Los cañones de sonido o dispositivos LRAD (*Long Range Acoustic Device*), operan en el rango audible (entre 2.000 y 4.000 Hz) y emiten haces acústicos de alta energía para comunicarse, advertir o inhabilitar a una persona mediante el dolor; pueden dañar el oído o causar pérdida auditiva permanente a distancias cortas. Su uso principal es el control de multitudes o áreas. El ultrasonido no es audible por las personas con oídos menos sensibles debido a la pérdida de agudeza auditiva causada por la edad, por lo que en términos generales solo afecta a las personas más jóvenes[14].

La medida pasiva más eficaz contra las armas sónicas es, de nuevo, sencilla. Se trata de generalizar los auriculares de protección empleados contra las granadas *flash bang,* que se citaron anteriormente. Su reducción activa de ruidos atenúa de manera automática todos los sonidos por encima de 82 dB; además, el protector auditivo ha sido probado en la banda de frecuencias audibles comprendida entre los 125 y 8.000 Hz, demostrando que protege en toda ella, pero brindando una mayor atenuación cuanto mayor es la frecuencia (sonido más agudo). Por tanto, la protección contra los ultrasonidos estaría garantizada, debiendo mejorarse la protección contra armas sónicas de baja frecuencia.

8. Agentes incapacitantes químicos y biológicos

Clásicamente, los agentes químicos y biológicos empleados contra personas se dividen en agentes incapacitantes y letales, siendo su diferencia principal la capacidad de matar o incapacitar temporalmente al combatiente en función de sus efectos fisiopatológicos. Pero desde la aproximación conceptual de este capítulo hay que tomar el concepto de incapacitante en un sentido más amplio, máxime cuando algunos de ellos no están incluidos en la comúnmente conocida como Convención de Armas Químicas (CAQ).

Existen determinados agentes biológicos incapacitantes de origen natural (por ejemplo, todas las enfermedades que puedan sufrir los componentes de la fuerza desplegada), contra los que se deben cumplir las medidas de protección sanitaria establecidas (alimentación, higiene, quimiprofilaxis o inmunoprofilaxis, etc.) y los controles establecidos por el personal facultativo (del Cuerpo Militar de Sanidad) que, obviamente, no se van a tratar en esta publicación.

[14] Un ejemplo de LRAD es el sistema Mosquito británico, que emite sonidos de ultra alta frecuencia (19-20 kHz), tiene un alcance comprendido entre 30 y 120 m y sector de haz de solo 15º.

En cambio, sí deben tenerse en cuenta otro tipo de agentes, fundamentalmente sustancias químicas, pero también biológicas obtenidas a partir de procesos biotecnológicos, que entran de lleno en la capacidad no letal objeto de este capítulo. Entre ellas se puede encontrar una gran variedad de sustancias que afectan a la movilidad o con capacidad de inutilizar materiales, además de los efectos psicopatológicos directos por su acción excitante o relajante:

- Sustancias antitracción: espumas rápidas pegajosas, pegamentos o antiadhesivos, cuya función es obstruir la progresión o inmovilizar tanto personas como vehículos. Se trata únicamente de un gel muy resbaladizo que se dispersa sobre una superficie impidiendo que exista agarre sobre ella.
- Sustancias adhesivas que bloquean las partes móviles del armamento clásico y las transmisiones mecánicas de los vehículos.
- Agentes tranquilizantes o desagradables como agentes pestilentes, gases lacrimógenos como el clorobenzilideno malononitrilo (CS, es uno de los más empleados en el mundo hoy en día), o gases salpimentados que causan reducción del volumen respiratorio, náuseas y vómitos, con irritación de las mucosas, cierre de los ojos o tos o marcadores que permiten la identificación de individuos. No existe un antídoto efectivo ante la exposición al gas lacrimógeno y sus efectos pueden neutralizar a una persona durante unos treinta minutos. Para su difusión se emplean los sistemas ya descritos en el apartado de material de control de masas.
- La aplicación de la biotecnología y de la inteligencia artificial para el desarrollo de agentes incapacitantes es una realidad frente a la que tenemos que hacer un esfuerzo de preparación desde el punto de vista doctrinal y operativo, participando en el desarrollo de contramedidas frente a estas amenazas.
- Los avances en neurociencia y neurotecnología podrán ser aplicados con fines espurios para desarrollar tecnologías o sustancias que incapaciten al personal de manera temporal o permanente, debiendo hacer un esfuerzo de preparación para hacer frente a esta amenaza.
- Por último, los agentes depresores del sistema nervioso central, como drogas, anestésicos, relajantes, sedantes, etc. Sustancias que, en función de su naturaleza, no están contempladas por la CAQ y que suponen una amenaza contra la que debemos hacer, de nuevo, un importante esfuerzo de preparación.

Las medidas de protección contra las sustancias antitracción son las mismas que las empleadas contra los sistemas de control de masas, básicamente mantener la distancia de seguridad con el posible agresor e interponer una

barrera física entre ambos. En cuanto al empleo de gases incapacitantes, el uso del equipo de protección individual, así como la aplicación de primeros auxilios en caso de resultar afectado, resulta vital para recuperar la operatividad en el menor tiempo posible[15].

9. Conclusiones y recomendaciones

Para evitar que los miembros de nuestras Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad sufran los efectos de los diferentes sistemas no letales que pueden ser empleados por nuestros potenciales adversarios (y que han sido descritos de la forma más sencilla posible en este capítulo), se propone emplear el mismo principio que se usa contra los sistemas letales del moderno campo de batalla: «Que no te vean, que no te den, que no te maten».

Que no te vean: se debe ser invisible para la observación enemiga. Para ello se recomienda adoptar las siguientes medidas:

Seguir empleando las clásicas garitas de vigilancia en las instalaciones militares con capacidad de observar sin ser observado. En los vehículos se deben emplear estaciones de armas remotas, cuyos sistemas electroópticos de vigilancia y observación son teleoperados desde su interior, sin exponer a la tripulación a la observación o agresión del adversario. Si nuestros soldados despliegan pie a tierra, se deben emplear redes de enmascaramiento multiespectrales (que nos ocultan simultáneamente de todos los espectros actuales de observación: visual, térmico y radar) para evitar la observación aérea y pantallas portátiles para evitar la terrestre (como la TACRION). Si las medidas pasivas fallan, se deben emplear los artefactos fumígenos de ocultación (también multiespectrales) que pueden ser lanzados tanto desde los vehículos militares (de momento los policiales carecen de esa capacidad) como por el personal desembarcado.

Si te ven, que no te den: la mejor medida de protección que se recomienda adoptar vuelve a ser de nuevo una muy sencilla y barata: mantener una distancia de seguridad entre nuestro personal y los posibles agresores (unos 20 m), evitando que puedan acercarse al personal o a los vehículos con cualquier excusa. Para prevenirse contra potenciales agresiones con vehículos de motor, cada patrulla/elemento de seguridad debe contar con

[15] Ejemplos de medidas sencillas frente a una agresión con gas CS son:

- Preventiva, el evitar el uso de lentillas, llevando mejor gafas el personal que lo necesite.
- Primeros auxilios, enjuagarse los ojos durante al menos quince minutos con agua; de lo que se desprende otra sencilla y barata medida: llevar petacas o bidones de agua en todos los vehículos de patrulla militares y policiales.

alguna medida de detención rápida (por ejemplo, la clásica *spike strip*); y, por supuesto, también con un sistema C/UAV portátil. Contra los sistemas láser y armas de microondas, los cristales de las garitas y los vehículos (especialmente los de sus pilotos y conductores) deberán tener filtros protectores específicos. También útil frente a las armas láser, de microondas y sónicas, cuyo haz debe impactar de forma precisa en el objetivo, es mantenerse en movimiento el mayor tiempo posible para dificultar la puntería.

Si te dan, que no te neutralicen: en este caso, al tratarse de armamento no letal que busca producir daños reversibles en las personas, hemos cambiado el principio clásico, sustituyendo el «que no te maten» por «que no te neutralicen». La medida pasiva básica que se recomienda adoptar es dotar a todos los individuos con la adecuada protección individual: uniforme especial anti traumas con protección contra láser y armas de microondas (como ya se dijo anteriormente, podemos encontrar auténticos uniformes de combate en diferentes fuerzas armadas de países de nuestro entorno, pero, por el momento, ninguno incorpora este tipo de protecciones), guantes de combate, chaleco antibalas, casco, protección ocular con filtro anti láser, protecciones acústicas contra armas sónicas, máscara antigás reglamentaria y alertador de iluminación láser portátil. También es necesario aplicar las habituales medidas de extinción de incendios. Los sistemas electrónicos militares deberán seguir contando con jaulas Faraday para protegerse contra el EMP. Las garitas empleadas por el personal de seguridad deberán ser blindadas y con cristales protegidos contra las posibles amenazas (como ya se ha dicho); asimismo, los vehículos de las patrullas también serán preferentemente blindados y con las ventanillas protegidas.

10. Bibliografía

Jefatura de Adiestramiento y Doctrina de Infantería. (2010). Proyecto de investigación 103/09 Armas no letales en las pequeñas unidades de Infantería. Granada, DIDOM.

Jefatura de Adiestramiento y Doctrina de Infantería. (2020). Estudio temático tecnológico de materiales (ETTM) 20/03 Armas de energía dirigida. Radiofrecuencia. Haces de partículas. Sónicas. Granada, DIDOM.

Jefatura de Adiestramiento y Doctrina de Infantería. (2020). Estudio temático tecnológico de materiales (ETTM) 20/05 Armas de energía dirigida. Generalidades. Láser. Granada, DIDOM.

Capítulo 3

Impacto de la revolución Bio en la Protección de la Fuerza

Alberto Cique Moya

Resumen

Estamos asistiendo a una revolución biológica —revolución Bio— donde la biotecnología, la biología sintética o la inteligencia artificial, aplicada con fines ilícitos, incrementarán las amenazas a la Protección de la Fuerza. El avance en el conocimiento de la genética y el desarrollo de las técnicas de biología molecular permitieron desarrollar programas biológicos basados en estas técnicas, que aún hoy en día siguen vigentes e incluso se magnifican gracias a la aplicación de las herramientas de biología molecular, para así conseguir agentes biológicos más patógenos o más resistentes. Para ello se utilizaron plásmidos para hacer resistentes a los agentes biológicos frente a los tratamientos establecidos, se integraron genes de diseño para modificar las características de los agentes biológicos o ampliar la gama de hospedadores. Para hacer frente a estas amenazas, organizaciones civiles y militares han desarrollado iniciativas para reducir el peligro, resultando fundamental establecer un marco de colaboración y control internacional para reducirlo. Así las cosas, resulta fundamental potenciar la investigación y desarrollo en el campo de las contramedidas sanitarias para reducir el impacto de un incidente de origen provocado o accidental, además de potenciar las capacidades sanitarias militares para hacer frente a un incidente de estas características.

Palabras clave

Biorrevolución, Biotecnología, Biología Sintética, Inteligencia artificial, Protección de la Fuerza.

The Impact of the biorevolution on Force Protection

Abstract

We are witnessing a biological revolution —bio revolution— where biotechnology, synthetic biology or artificial intelligence, applied for illicit purposes will increase the threats to Force Protection. Advances in the knowledge of genetics and the development of molecular biology techniques allowed the development of biological programs based on these techniques, which are still in force today and are even magnified by the application of molecular biology tools, in order to obtain more pathogenic and resistant biological agents. To this end, plasmids were used to make the biological agents resistant to established treatments, and designer genes were integrated to modify the characteristics of the biological agents or to expand the host range. To face these threats, civil and military organizations have developed initiatives to reduce the danger, and it is essential to establish a framework of international cooperation and control to reduce it. It is essential to promote research and development in the field of health countermeasures to reduce the impact of an incident of provoked or accidental origin, in addition to enhancing military health capabilities to deal with such an incident.

Keywords

Biorevolution, Biotechnology, Synthetic Biology, Artificial Intelligence, Force Protection.

1. Introducción

Desde siempre ha habido un interés en los conflictos por el uso de armas que generasen una ventaja táctica o estratégica. El desarrollo de las armas químicas o biológicas está sobradamente documentado históricamente, su uso ha sido abundante. A pesar de las iniciativas que trataban de evitarlo, el empleo de dichas armas se ha realizado la mayoría de las veces desde una aproximación empírica, por su contribución a la mejora del conocimiento científico.

Muchos son los ejemplos del empleo de este tipo de armas, solas o en combinación con otras tácticas a lo largo de la historia. Así, Aníbal ordenó arrojar vasijas cargadas con serpientes sobre los barcos del rey de Pérgamo con el objetivo de obtener ventaja táctica y libertad de acción; siglos antes, el griego Solón, durante el sitio de la ciudad de Cirra, aconsejó recoger plantas de eléboro para arrojarlas en el agua que sería consumida por los defensores de la misma, siendo este un ejemplo de utilización de dos tácticas execrables por las leyes y usos de la guerra actuales. Por un lado, la realización de modificaciones ambientales con fines militares, es decir, la alteración del curso del canal que proporcionaba agua a la ciudad y por otro, tras contaminar el agua con el eléboro, la reconducción del agua para que los sedientos sitiados cayeran enfermos tras consumirla y así poder tomar la ciudad sin resistencia.

Con el desarrollo de la microbiología, la proliferación biológica dio un salto enorme, pasando de una utilización que normalmente era de tipo puntual y con fines criminales, a un potencial empleo militar, principalmente de carácter estratégico, derivado del desarrollo de programas biológicos encubiertos, bajo la cobertura de programas declarados de investigación científica, es decir, de uso dual.

Esta posibilidad justificaba, a juicio de George W. Merck, la necesidad de que los EE. UU. continuaran con un programa biológico de carácter «eminentemente» defensivo que incluía bacterias, virus, hongos protozoos, toxinas de origen vegetal, bacteriano, fúngica o animal (incluidos venenos de serpientes) (Merck, 1945).

De manera análoga, los avances de la química abrieron el camino a la producción industrial de sustancias tóxicas, que han sido utilizadas de manera profusa y a gran escala en conflictos armados a partir del siglo XX, incluso a pesar de la existencia de normas de carácter moral y tratados internacionales que las han prohibido a lo largo de la historia. Situación que sin duda se verá más agravada con la aplicación de la inteligencia artificial generativa para el desarrollo de nuevas sustancias químicas tóxicas que incrementarán la amenaza en gran medida.

Los avances en cristalografía de rayos X permitieron desarrollar el modelo de doble hélice de la cadena de ADN, abriendo así la vía a profundizar en el estudio de la genética como ciencia básica y aplicada. A este respecto, Joshua Lederberg, en un artículo titulado «Swift biological advance can be bent to genocide», publicado en el *Washington Post,* el 17 de agosto de 1968, exponía que: «El pensamiento más escalofriante es que la investigación en Guerra Biológica apenas ha comenzado a aprovechar el potencial que ofrece la genética química para la construcción sistemática de nuevos agentes de enfermedades» (Lederberg, 1968).

Lederberg hacía un llamamiento a la necesidad de establecer un marco regulatorio efectivo para impedir el desarrollo de programas biológicos ofensivos y la necesidad de prepararse frente a ellos, ya que la amenaza era real. Asimismo, recalcaba los peligros que entrañaban los avances en el conocimiento del código genético a efectos de desarrollar «armas virales antihumanas», exponiendo a juicio público la siguiente opinión: «Puede que estemos en el umbral de una tecnología de incalculable importancia en medicina diagnóstica y terapéutica..., si tenemos el coraje de seguir adelante a pesar de los riesgos que implica» (Lederberg, 1975a).

El descubrimiento en 1952 del papel de los plásmidos en la resistencia bacteriana a los antibióticos fue aprovechado en los años posteriores con fines espurios por dos vías diferenciadas. Por un lado, para seleccionar agentes biológicos que de forma natural eran resistentes a determinados antibióticos; mientras que, por el otro, se introdujeron plásmidos de resistencia antibiótica específicos a microorganismos que de forma natural eran sensibles al mismo (Price *et al.,* 2003).

La importancia del desarrollo de este tipo de agentes biológicos modificados era y es, como se ha podido leer en la cita anterior, determinante para la Protección de la Fuerza, ya que, incluso hasta los años noventa, los tratamientos antibióticos establecidos en los manuales médicos civiles serían inefectivos en caso de diseminación de este tipo de agentes. Sirva de ejemplo la recomendación incluida en los manuales militares de administrar ciprofloxacina o doxiciclina para hacer frente al *Bacillus anthracis*, mientras que en los libros civiles el tratamiento recomendado era la penicilina, teniendo que esperar al Amerithrax o «crisis de los sobres» para que se modificaran todas las guías terapéuticas y protocolos de actuación aprovechando el conocimiento militar.

La alteración de las resistencias antibióticas no era la única preocupación expresada por la Organización Mundial de la Salud, que ya mostró su inquietud ante el potencial que tenía la revolución biotecnológica que se estaba produciendo a nivel mundial en lo referente al incremento de la amenaza biológica. De hecho, en la época de Brezhnev el programa

biológico soviético cambió su orientación al abandonar la microbiología clásica en favor de la ingeniería genética, iniciándose así la segunda generación del programa bajo la cobertura de Biopreparat con el objetivo de (Rimmington, 2021):

- Producir «mejores» y diferentes microorganismos gracias a la alteración e incremento de la virulencia y de la inefectividad de los agentes biológicos.
- «Cambiar» propiedades de la superficie de virus y bacterias (determinantes antigénicos), a efectos de dificultar/impedir su detección o identificación.
- Disminuir o alterar la sensibilidad antibiótica o a las vacunas.
- Incrementar la resistencia ambiental de los agentes biológicos.

Desde otra aproximación conceptual, siendo el cognitivo el quinto ámbito de operación, es necesario traer a colación la posibilidad, más allá de la aplicación de técnicas asociadas a la neurociencia o la neurotecnología, de poder actuar de manera directa sobre la mente utilizando agentes biológicos o químicos con la intención de alterar los procesos cognitivos del enemigo en un contexto de guerra cognitiva.

A este respecto, el ya mencionado Joshua Lederberg hacía mención expresa a la amenaza que supondría enfrentarse a agentes biológicos con efectos mentales, a los que denominaba *hypno-virus*, haciendo una analogía expresa al empleo de sustancias químicas que afectaban a la mente o que trataban de controlarla como una amenaza asociada a la guerra biológica, es decir, agentes químicos o biológicos empleados en lo que podría llamarse en su sentido más amplio «guerra cognitiva». Sirvan de ejemplo los experimentos de control mental llevados a cabo por los EE. UU. durante la Guerra Fría, bajo el nombre en clave Proyecto MKUltra, en los que se incluían diferentes aproximaciones conceptuales, más allá de uso de drogas como el LSD, con el objetivo de investigar y desarrollar agentes químicos, biológicos o materiales radiológicos para ser empleados en operaciones clandestinas de control del comportamiento humano (Gross, 2019).

No puede finalizarse esta introducción sin citar los escenarios más probables de empleo de agentes biológicos, modificados o no, referido a los EE. UU. en 2002, pero asumible para el resto en el entorno actual de inseguridad existente, destacando entre ellos el escenario agro terrorista (dirigido contra la cabaña ganadera fundamentalmente), un ataque bioterrorista contra tropas desplegadas, incluidas las aliadas, en Oriente Próximo y una diseminación urbana intencionada en una ciudad norteamericana o de un país aliado.

En el marco de los biomateriales obtenidos mediante la biotecnología, podríamos añadir a los escenarios anteriores el uso de agentes biológicos e incluso químicos que causaran deterioro de los materiales, incluso en los equipos de protección corporal y respiratoria, entre otros muchos, para que a modo de gases rompe-máscaras deterioraran el material de los filtros permitiendo la entrada de otro agente en una segunda diseminación.

Lamentablemente, el desarrollo de la biotecnología, la mejora y simplificación de las técnicas de ingeniería genética en conjunción o no con la inteligencia artificial generativa, la bioinformática y la biología sintética, así como las ciencias ómicas[1], no solo se aplican para el progreso humano, sino que pueden ser aprovechadas con fines espurios para obtener agentes químicos o biológicos que puedan ser utilizados en un contexto de guerra biológica o de bioterrorismo. Esta posibilidad nos obliga a hacer un esfuerzo de preparación, ya que, aunque el impacto epidemiológico de su empleo fuera reducido, el impacto en el ámbito cognitivo sería brutal.

Asimismo, en relación con el ámbito cognitivo de las operaciones, no hay que olvidar el lanzamiento de campañas de desinformación que magnifiquen las amenazas. Resultando fundamental no solo disponer de contramedidas sanitarias, sino que habría que disponer de personal experto que haga las pertinentes evaluaciones de la amenaza (Rosenzweig, 2022).

2. La revolución Bio ¿un reto para la seguridad?

La pandemia de la COVID-19 ha traído a nuestras mentes la importancia de los avances en la ciencia biológica, en confluencia con otras ciencias y tecnologías, para cambiar el mundo tal y como lo conocíamos. Desde acabar con las enfermedades hasta terminar con la inseguridad alimentaria, pasando por hacer este mundo más sostenible en el marco de una revolución biológica, aún en ciernes, donde los beneficios de la misma no nos pueden hacer olvidar los riesgos que pueden entrañar para la seguridad, hecho que ya era contemplado en la Estrategia de Seguridad Nacional de 2011.

A efectos de destacar la importancia que la biotecnología, la ingeniería genética y la biología sintética tendrán en el ámbito de la seguridad y la defensa en un futuro más o menos inmediato, solo hay que recordar las afirmaciones realizadas en 2015 por el presidente de la Academia China de Ciencias Médicas Militares en el sentido de que la «biotecnología se convertirá en el

[1] Las ciencias ómicas incluían la genómica, la transcriptómica, la proteómica, la epigenómica y la citómica, incluyéndose en la actualidad otras como la farmacogénomica, la nutrigenómica, la metabolómica, la lipidómica, la secretómica, la interactómica, la fenómica, la exposómica, la metagenómica y la microbiómica. Disponible en: https://www.institutoroche.es/static/archivos/Informes_anticipando_CIENCIAS_OMICAS.pdf

nuevo «mando estratégico» de la defensa nacional, desde los biomateriales hasta las armas de «control cerebral» (Kania y Vorndick, 2019).

Profundizando en esta aproximación militar y no solo en respuesta a los riesgos de las enfermedades infecciosas, China ha declarado su interés en «explorar el potencial militar e incluso las aplicaciones ofensivas de la biotecnología», ya que «La biotecnología moderna y su integración con la información, la nanotecnología, el ámbito cognitivo, etc., tendrán una influencia revolucionaria en las armas y equipos, los espacios de combate, las formas de guerra y las teorías militares».

El interés militar chino demostrado por alcanzar ese «dominio biológico» es tal que en la política china de fusión civil y militar se destaca a la biología como una prioridad para convertirse en el líder mundial de la biotecnología (Mayfield, 2020), para lo que considera prioritario promover el desarrollo innovador de la bioeconomía a fin de acelerar el desarrollo de la sanidad, la agricultura, la energía, el medioambiente y la bioinformática. Todo ello con el fin último de participar activamente en la gobernanza global de bioseguridad, con un espíritu colaborativo a nivel internacional y multilateral, tal como se incluye en el 14.º Plan quinquenal 2021-2025 de la Asamblea Popular Nacional de la República Popular China (Shijia, 2022).

Para corroborar ese interés político-militar hay que tener en cuenta que, aunque EE. UU. continúa liderando el sector biotecnológico a nivel mundial, China esta haciendo un esfuerzo por reducir esa diferencia en investigación básica y aplicada (Salitskii y Salitskaya, 2022):

- Respecto al número de publicaciones, China aumentó un 20 % anual en el periodo comprendido entre 2007 y 2017, alcanzando el 14 % del total mundial en ciencias de la salud en 2019.
- En relación con el número de patentes biotecnológicas, China pasó del 1 % en el año 2000 hasta el 28 % en 2019. En comparación, EE. UU. sufrió una regresión en el mismo periodo del 45 al 27 %, resultando fundamental tener en cuenta en la lectura de estos datos que EE. UU. copa el primer puesto a nivel mundial en patentes de tipo internacional frente a las exclusivamente nacionales chinas.
- El ámbito cognitivo (neurotecnología y neurociencia) y el sector sanitario forman parte de los megaprogramas de ciencia e ingeniería establecidos.
- Por otro lado, en relación con la producción mundial de productos farmacéuticos, China ha incrementado su participación del 7 al 22 % en el periodo 2011-2021, representando el 40 % del sector biofarmacéutico mundial, lo que es relevante desde el punto de vista de disponibilidad y acceso a determinadas contramedidas sanitarias en situaciones de emergencia, circunstancia que debe de ser tenida en cuenta a los efectos de

disminuir nuestra dependencia exterior y mantener un depósito de contramedidas sanitarias para hacer frente a una posible necesidad.

Todos estos datos muestran una carrera brutal en el ámbito económico, político, científico y geoestratégico, que influye sin ninguna duda en el entorno de seguridad, donde en numerosas ocasiones es difícil de establecer la barrera entre lo ético o lo moral con lo legal, siendo el ejemplo paradigmático de este reto los primeros bebés modificados genéticamente por el investigador chino He Jiankui, el que eliminó, aplicando la técnica de edición genética CRISPR[2], el gen CCR5 de tres embriones con el objetivo de hacerlos resistentes al VIH, la viruela y el cólera.

Esta noticia hizo saltar las alarmas a nivel mundial y provocó que las autoridades chinas le condenaran a tres años de prisión por haber vulnerado las leyes, planteándose la posibilidad, más allá de los beneficios potenciales, de que este tipo de experimentos, alejados de toda ética científica, abran la puerta incluso a programas de eugenesia con fines militares en caso de ser aplicados a gran escala (Bollero, 2018).

El impacto brutal que ha provocado la pandemia no nos puede hacer olvidar que ha permitido, pero también obligado, aprovechar las sinergias existentes y tratar de reducir nuestra dependencia en sectores críticos con un impacto en la seguridad, más ahora cuando asistimos a un salto cualitativo y cuantitativo que esta transformando nuestra sociedad gracias al desarrollo de la revolución de la información.

Dicha transformación tendrá como aspectos positivos un impacto beneficioso en la salud, bienestar y protección ocupacional del soldado, pero también un impacto negativo derivado de los cambios geoestratégicos a nivel local, regional y global, así como del mal uso o la mala aplicación de estas tecnologías que seguro darán lugar a nuevos riesgos y amenazas, principalmente referidos a las amenazas difusas en un contexto de zona gris.

La interacción sinérgica derivada del desarrollo de diferentes tecnologías y ciencias en un contexto de revolución Bio incluyen desde la biotecnología a la biología sintética, pasando por la neurotecnología, las ciencias computacionales o la inteligencia artificial (IA), todo ello relacionado con

[2] El acrónimo CRISPR, Clustered Regularly Interspaced Short Palindromic Repeats (Repeticiones Palindrómicas Cortas Agrupadas y Regularmente Interespaciadas), es la denominación de unas secuencias repetitivas presentes en el ADN de las bacterias de virus que les habían infectado en el pasado, facilitando su reconocimiento en nuevas infecciones para defenderse frente a ellos cortando su ADN. Para ello, utiliza unas guías y una proteína (Cas9) para dirigirse a zonas elegidas del ADN y «cortar**»**. A partir de ahí, se pueden pegar los extremos cortados e «inactivar» el gen, o introducir moldes de ADN, lo que permite «editar» sus «letras» a voluntad. Disponible en: (https://www.agenciasinc.es/Reportajes/El-editor-genetico-CRISPR-explicado-para-principiantes)

la transición desde el Internet de las Cosas (IoT) hacia el Internet de los Cuerpos (IoB). Esto es debido fundamentalmente al incremento de la utilización de dispositivos, integrados o no, que monitorizan a los individuos y transmiten la información a través de las redes de comunicación, permitiendo en el campo militar mejorar la conciencia situacional. Sin embargo, hay que tener en cuenta que esta información, por su carácter crítico, debe de ser protegida para evitar sea conocida y explotada por el oponente, confiriéndole una ventaja en todos los niveles de las operaciones, máxime con el desarrollo de la computación cuántica y la aplicación de algoritmos de inteligencia artificial (IA) o *big data* (Lee *et al.,* 2020).

3. Del programa biológico soviético a la biología sintética

A pesar de que en un trabajo de prospectiva parecería atrevido hacer énfasis en algo pasado, no resulta descabellado analizar las líneas de trabajo de la segunda generación del programa biológico soviético, ya que no solo coinciden con las actuales, sino que se ven magnificadas en función del desarrollo de la biotecnología y la biología sintética o la inteligencia artificial, circunstancia que podrá afectar sin ninguna duda a la Protección de la Fuerza (Almosara, 2010).

La falta de gobernanza existente y la carencia de una herramienta de verificación de la vulgarmente conocida como Convención de Armas Biológicas y Toxínicas (CABT) provoca que el peligro se incremente, situación que se agrava aún más si cabe por la democratización del conocimiento, la simplificación de las técnicas y la reducción de costes asociada a la revolución Bio.

De ahí la importancia de potenciar los controles internacionales de carácter cooperativo para prevenir la difusión de tecnologías y materiales susceptibles de promover el desarrollo o la adquisición por parte de Estados y terroristas de armas químicas y biológicas (Hidalgo García, 2016).

Esa «facilidad de acceso» a agentes químicos o biológicos debe de tenerse en cuenta en todos los niveles de las operaciones, resultando fundamental establecer una estrategia de biopreparación y biorrespuesta que contemple todos estos aspectos con el objetivo último de proteger al combatiente frente a la amenaza o empleo de estos agentes.

3.1. Desarrollo de armas biológicas binarias

A semejanza de las armas químicas binarias[3], un arma biológica binaria consta de un sistema diseminador que contiene dos agentes biológicos

[3] Las armas químicas binarias se componen de un sistema diseminador con dos sustancias químicas no tóxicas que al mezclarse se transforman en tóxicas.

independientes que al combinarse incrementan su peligrosidad, o que son preparados antes de ser «cargados» en el dispositivo de diseminación (Wickiser *et al.,* 2020).

El conocimiento de los mecanismos moleculares relacionados con la patogenicidad y la interacción entre diferentes microorganismos permitirá disponer de este tipo de agentes binarios, aprovechando sinergias entre microorganismos para incrementar la gravedad del cuadro clínico de uno de ellos.

Los virus de las hepatitis D y B, obviando aspectos relacionados con el periodo de incubación y el mecanismo de infección, pueden ser un ejemplo de agentes biológicos binarios. Esto es así porque el virus de la hepatitis D requiere la presencia del virus de la hepatitis B para replicarse, empeorando generalmente los síntomas de la hepatitis B (Giersch y Dandri, 2015).

El efecto patógeno del *Bacillus cereus,* normalmente asociado a toxiinfecciones alimentarias, se basa en dos toxinas termoestables, la toxina diarreica y la emética, pero en caso de integrar, de manera natural o intencionada, los plásmidos PX01 y PX02, la bacteria será más patógena porque incrementará su capacidad de producción de toxinas (factor letal, factor edema y factor necrotizante) y porque generará una cápsula que le protegerá de la fagocitosis. Por añadidura, puede incrementarse su resistencia a diferentes antibióticos, incluso a elevadas concentraciones de ciprofloxacina (Vicki *et al.,* 2006).

En relación con los agentes biológicos binarios, es necesario destacar la importancia del periodo de incubación y la aparición de los efectos que provocan, así como la complejidad técnica necesaria para poder «integrar y expresar» en el microorganismo receptor las características patogénicas del donante, circunstancia que no ocurre con las armas químicas binarias, ya que el proceso es inmediato.

3.2. Integración de genes de diseño en genoma de agentes biológicos

De las muchas noticias que sucedieron en 2001, destaca por su relación con este apartado, el experimento fallido de edición genética realizado por un grupo de investigación australiano que generó la intervención del gobierno.

Los investigadores trabajaban con el virus ectromelia (virus de la viruela del ratón) para estudiar la viabilidad del control de poblaciones de roedores. Para ello, insertaron el gen de la interleukina 4 en el virus para que al expresarse en las hembras impidiera la anidación de los embriones en el útero. A efectos de comprobar la seguridad y efectividad del ensayo, inocularon el virus modificado en dos lotes de ratones, uno de los cuales había

sido vacunado frente a la viruela, dando como resultado del experimento la muerte de todos los animales. La investigación posterior determinó que la interleukina 4, aparte de ese efecto buscado, suprimía la respuesta inmunitaria (Jackson *et al.,* 2001).

Como consecuencia inmediata, se informó del incidente a las autoridades australianas, las cuales a su vez lo notificaron a la CABT por las implicaciones derivadas del experimento, que no eran otras que se pudiera sospechar que el ensayo formaba parte de un programa biológico en el marco de un programa de uso dual.

La lección identificada de este experimento se relaciona con la necesidad de analizar y conocer en profundidad el mecanismo biológico en el que se quiere intervenir. De ahí la necesidad de aplicar el principio de precaución y de tener en consideración los peligros de intervenir en líneas somáticas y germinales que la aplicación de la tecnología de edición genética permite.

Hasta la aparición del CRISPR, junto con otros impulsores genéticos o *gene drives*, la posibilidad de modificar el genoma de manera eficiente era reducida por la falta de sensibilidad de las técnicas utilizadas. Pero con el desarrollo de esta tecnología, en conjunción con el mayor conocimiento del genoma y de las funciones de los genes, el inicio de la medicina de precisión ha dado un salto cualitativo y cuantitativo formidable; de ahí, por ejemplo, la aplicación de la terapia génica con el objetivo de sustituir a nivel celular genes defectuosos por genes sanos para curar una enfermedad genética, baste recordar los avances en el tratamiento de la talasemia, entre otras enfermedades, para corroborarlo (Hunt, 2023).

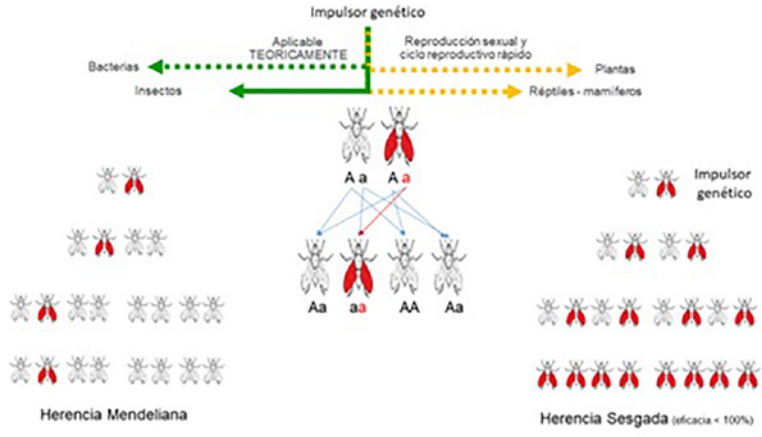


Figura 1. Efecto de los impulsores genéticos sobre la herencia

El uso de impulsores genéticos permite, al menos en teoría, modificar la genética de poblaciones enteras (siempre teniendo en cuenta sus ciclos reproductivos), ya que el impulsor genético se impone ventajosamente por medio de la reproducción sexual a través de una población de organismos, transmitiendo un rasgo genético particular a toda o a la mayoría de su descendencia gracias a la herencia sesgada en contraposición a la herencia mendeliana en lo que se denomina «reproducción egoísta» (Figura 1) (Henn y Imken, 2022).

Figura 2. Tipos de impulsores genéticos

En el momento actual, los impulsores genéticos solo pueden funcionar en organismos huésped de reproducción sexual y un ciclo reproductivo rápido, pudiendo aplicarse conceptualmente en dos vías: la primera, como tecnologías de extinción genética y la segunda, como estrategias de biocontrol genético.

Teóricamente, se distinguen diferentes tipos de impulsores en función de la acción que realizan, desde impulsores globales que continuarían esparciéndose hasta que resultara afectada la especie a nivel global hasta los impulsores sensibilizadores que hacen a un organismo más sensible a un estímulo externo (Figura 2).

La utilización de esta tecnología sin adoptar las adecuadas precauciones tiene una importancia en la seguridad a nivel global. Esto es así porque la aplicación de estos impulsores en el contexto de biología sintética y biosíntesis, en conjunción con la aplicación de la inteligencia artificial en plantas o en insectos podría, en el peor escenario posible, tener consecuencias calamitosas para el mundo tal y como lo conocemos.

No se pueden dejar de citar los intereses no solo comerciales que estan detrás del desarrollo de esta «nueva tecnología, potente y peligrosa. Su

potencial como arma biológica que podría tener impactos desastrosos sobre la paz, la soberanía alimentaria y el ambiente», pero también su efecto beneficioso en el combate de las enfermedades, etc. (Group, 2017).

Si obviamos las aplicaciones beneficiosas en la agricultura/ganadería relacionadas con la seguridad alimentaria, tenemos que ser conscientes de los efectos perjudiciales relacionados con el fortalecimiento de los monopolios comerciales, lo que podrá afectar al clima de seguridad internacional.

La disminución de las enfermedades transmitidas por vectores es otro posible beneficio, pero tenemos que ser conscientes de los efectos derivados de alterar el equilibrio ecológico que suponga una amenaza a la biodiversidad. Y por último, pero no menos importante, aplicar esta tecnología para eliminar especies invasoras, conocimiento que puede entrar de lleno en la investigación de uso dual y el desarrollo de agentes biológicos. Todo esto determina la necesidad de un marco de gobernanza a nivel mundial que permita optimizar los beneficios y anular los perjuicios.

Las cuestiones éticas y morales derivadas de la modificación de líneas somáticas y germinales plantean discusiones encendidas acerca de la aplicación de estas técnicas cuando no se conocen las implicaciones que pueden tener esas manipulaciones en el conjunto del genoma y su expresión posterior, planteándose desde el punto de vista de la seguridad escenarios apocalípticos derivados de la aplicación a gran escala de estas técnicas en programas de eugenesia dirigida, ya sea para «desarrollar/crear supersoldados» o poblaciones diferenciadas por características raciales en función de la manipulación a la que fueran sometidos sus progenitores, o incluso enfrentarnos a hombres-máquina (Dilanian, 2020).

La aplicación práctica de las teorías transhumanistas no es ajena a esta posibilidad. Esto es así porque podría plantearse que algún *biohacker* tuviera la capacidad de llevarla a cabo, dentro del concepto del «Nuevo Hombre», aplicando herramientas genéticas en conjunción o no con técnicas de neurotecnología (Mendz y Cook, 2021).

3.3. Creación de virus silentes

El arma biológica es, a diferencia del arma química, un arma de carácter estratégico, fruto de ese uso puede plantearse la posibilidad, en función del desarrollo científico, de que se desarrollen agentes biológicos, idealmente de carácter transmisible, que infecten a un individuo y no le provoquen enfermedad, infectando a la población objetivo conforme pasa el tiempo y no expresándose, es decir, no desarrollándose la enfermedad, en tanto en cuanto no son activados por el desencadenante específico cuando así sea considerado.

Esto que parece irreal sucede en la naturaleza de manera natural, de hecho, nuestro genoma humano (así como de la gran mayoría de las células eucariotas) contiene una gran proporción de retrovirus endógenos humanos (HERV), que no son otra cosa que fragmentos de secuencias de virus que alguna vez a lo largo de la evolución infectaron al ser humano, insertándose de manera permanente en el genoma (Sentís, 2002).

El virus SARS-CoV-2 es un ejemplo de cómo un estímulo (un virus) puede «despertar» retrovirus latentes en el organismo provocando una reacción inflamatoria anormal, junto con una disminución en el número de linfocitos. Pero no solo el virus en sí es capaz de provocar una respuesta, sino que se ha descrito que individuos vacunados frente a la COVID-19 han sufrido la reactivación de virus de la varicela zóster (Charvet *et al.,* 2023).

Sin ánimo de entrar en disquisiciones metafísicas, la posibilidad de desarrollar inmunomoduladores o biorreguladores a la carta que activarán procesos o mecanismos que culminarán en una enfermedad, abre la posibilidad de que este escenario fuera más propio del empleo selectivo de agentes biológicos contra objetivos determinados, que de emplearlo contra los efectivos desplegados en un área de operaciones, ya que el periodo de latencia entre la activación y el desarrollo del cuadro clínico sería largo en el tiempo. No obstante, no se puede olvidar el carácter estratégico del arma biológica planteado anteriormente.

A modo de ejemplo exclusivamente teórico, puede plantearle el efecto que tendría disponer de una sustancia que activara alguno de los genes RAS, incluido en el grupo de los oncogenes, como pudiera ser el gen KRAS que diera lugar a la generación de neoplasias en diferentes órganos y sistemas[4].

3.4. Ampliar la gama de hospedadores

Los polémicos experimentos de ganancia de función permiten, entre otras posibilidades, ampliar la gama de hospedadores (mejorar la susceptibilidad de un hospedador ante un agente o toxina), incrementar la transmisibilidad o patogenicidad, así como la posibilidad de eludir las contramedidas médicas (Warmbrod *et al.,* 2021).

Obviando los claros beneficios que generan los experimentos de ganancia de función en cuanto al mejor conocimiento de los agentes biológicos, no puede dejar de citarse que esa alteración y mejora de determinados agentes biológicos suponen un riesgo para la seguridad y la salud global,

[4] El gen KRAS da origen a una proteína que participa en las vías de señalización celular que controlan la formación, maduración y destrucción de las células, es decir, pueden encontrarse en algunos tipos de cáncer. Disponible en: https://www.cancer.gov/espanol/publicaciones/diccionarios/diccionario-cancer/def/gen-kras-natural

especialmente cuando ese conocimiento se difunde de manera libre a través de publicaciones científicas con el objetivo altruista del avance de la ciencia y la mejora del conocimiento (Yanes, 2023).

Esta postura fue la que provocó que las autoridades estadounidenses trataran de impedir en 2012 la publicación de dos trabajos donde se explicaba con detalle cómo lograr modificar el genoma del virus de la gripe aviar H5N1 para que fuera transmisible al hurón, estableciendo seguidamente una moratoria de tres años donde se instaba a no realizar ningún tipo de experimento de ganancia de función (Masaki *et al.,* 2012; Herfst *et al.,* 2012).

Pasado ese tiempo y en vista de que este tipo de experimentos mejoraba el conocimiento en lo relativo a desarrollo de tratamientos y vacunas, se estableció un programa para que, en caso de que los investigadores quisieran recibir financiación de los agentes biológicos incluidos en el listado de agentes seleccionados (virus, bacterias y toxinas), que afectan al ser humano, a los animales y a las plantas, debían ser sometidos a evaluación (Centers for Disease Control and Prevention and Animal and Plant Health Inspection Service, 2023).

La polémica respecto a los experimentos de ganancia de función y su relación con las medidas de bioseguridad necesarias para evitar accidentes, volvió a resurgir con el SARS-CoV-2, fundamentalmente debido a la difusión de teorías conspiranoicas, generadas por intereses políticos o de grupos de presión, relativas a su posible origen en el laboratorio, aunque esto no nos puede hacer olvidar que hoy en día, con la información disponible, las evidencias científicas, a pesar de la mejorable colaboración de las autoridades chinas, conducen a considerar el origen natural frente al provocado o accidental (*The Lancet Microbe*, 2022; Farkas *et al.,* 2023; Pagani *et al.,* 2023).

Lo anterior tiene una importancia capital en las operaciones y en la Protección de la Fuerza, ya que disponer de capacidades sanitarias militares resulta clave para la investigación y adopción de medidas de control, incluso en ambiente no cooperativo cuando así sea determinado. Asociado a esto, no puede olvidarse la importancia de la comunicación estratégica en este tipo de situaciones a efectos de difundir mensajes claros y veraces. La formación e instrucción del personal resulta clave para el cumplimiento de las normas establecidas de protección sanitaria de la fuerza, además de mejorar la adherencia a los tratamientos quimio e inmunoprofilácticos.

La falta de bioseguridad de las instalaciones y la falta de ética del personal investigador hacen de los experimentos de ganancia de función uno de los riesgos más graves a los que nos enfrentamos. Si a esto unimos que sean la base de un programa biológico por parte de actores estatales y no estatales, la amenaza es mucho mayor. De ahí la importancia del establecimiento

de una gobernanza efectiva global y la necesidad de preparación para hacer frente a brotes de enfermedad (López Baroni, 2015).

Desde otra aproximación conceptual, la mejora del conocimiento de los mecanismos genéticos podría permitir modificar microorganismos no patógenos para el hombre en patógenos, transformándolos en «microorganismos humanizados» mediante la eliminación del sesgo de codón, permitiendo así el salto interespecies (Woo *et al*., 2009).

3.5. Desarrollo de agentes biológicos de diseño

Los avances en la síntesis y la secuenciación de los ácidos nucleicos permiten modificar de manera deliberada el genoma de los microorganismos, llegando incluso a sintetizarlo por completo gracias a la biología sintética (Sharma *et al.,* 2020).

En 2011, la secretaria de Sanidad y Servicios Sociales norteamericana, Kathleen Sebelius, refiriéndose a la necesidad de una moratoria para la destrucción del virus de la viruela declaró: «[…] the virus' genomic information is available online and the technology now exists for someone with the right tools and the wrong intentions to create a new smallpox virus in a laboratory» (Sebelius, 2011).

Pocos años después fue sintetizado el virus de la viruela del caballo por poco más de 100.000 $, planteándose si este tipo de experimentos, más allá de lo declarado, tenían beneficios para la salud pública (Kupferschimdt, 2017).

La aplicación de la tecnología de impulsores genéticos en programas biológicos constituye una de las principales amenazas a las que nos enfrentamos, no solo por la posibilidad de alterar el equilibrio ecológico, sino por la posibilidad de tratar de obtener «armas étnicas» que afectaran exclusivamente a un grupo de población, enfrentándonos entonces a un programa de eugenesia a gran escala.

> «[…] the most serious threat to our security may consist of unannounced attacks on American cities by sub-national groups using genetically engineered pathogens. The acquisition of bioweapons and biotechnology is becoming easier as technology spreads and advanced scientific techniques become more accessible globally […]» (Committe on Armed Services House of Representatives, 1999).

Desde otra aproximación, la optimización de las técnicas de hibridación y de inserción genética permitiría obtener agentes biológicos con capacidad de síntesis o expresión de toxinas, biorreguladores o moduladores. Para

ello, sería necesario conocer el proceso biosintético y la ruta metabólica que culminara en la producción de ese tipo de sustancias. Llevando más allá ese planteamiento, podría contemplarse, en caso de conocer el gen que codifica una sustancia endógena, biorregulador o modulador, la posibilidad de insertarlo en un microorganismo, generalmente una bacteria o un hongo, para que conforme se desarrollara iniciara una producción masiva del mismo. Otra posible línea de desarrollo de biorreguladores que pudieran utilizarse con fines bélicos o terroristas podrían obtenerse gracias a procesos biosintéticos, aplicando o no, algoritmos de inteligencia artificial.

Los biorreguladores o moduladores son compuestos orgánicos que regulan distintos procesos celulares, en los cuales se incluyen citoquinas, eicosanoides, neurotransmisores, hormonas o enzimas proteolíticas. A diferencia de los agentes biológicos clásicos (agentes biológicos vivos y toxinas), que precisan de un periodo de incubación o de latencia para iniciar su efecto, los biorreguladores tienen un efecto inmediato tras su ingreso en la economía orgánica (Kagan, 2006).

En función del biorregulador obtenido se afectaría uno o varios sistemas orgánicos, desde el sistema nervioso hasta el inmunitario. Respecto a los que afectaran al sistema nervioso, se podría alterar desde el estado de ánimo hasta dañar el sistema nervioso, lo que entraría en el ámbito de guerra cognitiva. El desarrollo de la neurociencia ha incrementado la posibilidad de empleo de este tipo de sustancias, por lo que resulta fundamental profundizar en el conocimiento de la neurociencia para desarrollar contramedidas que permitan hacer frente a esta amenaza (Bokan, 2005).

4. Desafíos de la ingeniería genética

A lo largo del texto se ha podido constatar de manera fehaciente como la ingeniería genética ha preocupado desde prácticamente sus inicios, no solo en organizaciones del ámbito de la defensa, caso de la Organización del Tratado del Atlántico Norte (OTAN), sino que preocupa en el campo de la salud, como es la Organización Mundial de la Salud o incluso en el campo de las organizaciones no gubernamentales como es el caso del Comité Internacional de la Cruz Roja y Media Luna Roja.

Todas esas organizaciones han mostrado y muestran una gran preocupación por disminuir la amenaza asociada a la ingeniería genética, o más recientemente la biología sintética o el *biohacking*, solas o por sus relaciones con la bioinformática o la inteligencia artificial generativa, desarrollando iniciativas y herramientas que tratan de evitar la proliferación de agentes biológicos tal cual han sido descritos anteriormente.

Para la OTAN, la amenaza de la biotecnología y de la biología sintética no se limita a los agentes biológicos clásicos, normalmente cubiertos por las regulaciones establecidas, sino que hace especial hincapié en aquellos que van dirigidos a los cambios de secuencia inducidos intencionadamente para eludir la Detección, Identificación y Monitorización (DIM), así como para dificultar el diagnóstico y el tratamiento establecido.

Un aspecto relevante para la OTAN esta asociado a la seguridad de los datos genéticos y su potencial relación con las posibles dianas genéticas que pudieran generar una vulnerabilidad de grupo (Blumenthal *et al.,* 2021). De ahí la importancia de controlar el intercambio de información y de las bases de datos en su relación con la inteligencia artificial y el *big data*, ya que lo más importante en esta revolución Bio es: ¿quién controla la información genética? Por otro lado, si esa información puede ser utilizada para la orientación genética.

Quizá por esa razón las autoridades militares norteamericanas aconsejaran a sus miembros no utilizar test de ADN que tenían que ser remitidos a China para su análisis con el objetivo de conocer sus ancestros. O las autoridades civiles mostraran su preocupación en relación con una empresa china ligada a la investigación militar que se sospechaba estan recolectando datos de mujeres norteamericanas (Needham y Baldwin, 2021), pero no solo las autoridades chinas pudieran estar recabando información genética de la población en general, sino que algunos países como Rusia o EE. UU. también estarían interesados en recabar este tipo de información, lo que explicaría por qué el presidente Macron no quisiera realizarse una PCR cuando se entrevistó con el presidente Putin o por qué los EE. UU. estarían interesados en recolectar información genética de líderes políticos (Reuters, 2022).

Esa interacción o integración de tecnologías, sin duda alguna de doble uso, podrán contribuir a alterar los equilibrios de poder y favorecer un empleo asimétrico en un contexto de zona gris, donde nuestras fuerzas deberán integrar todas esas nuevas herramientas que están por venir y que sin duda nos permitirán hacer frente a las amenazas futuras (Tucker, 2020).

Es importante resaltar, como una de las principales amenazas a las que tendremos que hacer frente, el uso malévolo de la IA o de la biología sintética, en conjunción con otras técnicas y ciencias, para el desarrollo de programas biológicos y químicos que permitan sintetizar o modificar agentes biológicos o químicos contra los que será preciso desarrollar contramedidas sanitarias para hacerlos frente, ya sean agentes incapacitantes o letales, a merced de disponer de capacidad de investigación en un contexto de

cooperación cívico-militar, ya que es y será nuestra seguridad la que se vea amenazada (Edwards, 2022).

Muchas de las tecnologías descritas a lo largo de este trabajo pueden ser utilizadas para la mejora del rendimiento del soldado, si bien, lamentablemente, como se ha expuesto, pueden ser utilizadas por nuestros adversarios con fines espurios, aunque entren en conflicto con el derecho internacional humanitario, las iniciativas internacionales y convenciones establecidas, con el objetivo de obtener «supersoldados» más resistentes o más inteligentes gracias a intervenciones médicas o biológicas o modificaciones genéticas, pero sin las cortapisas morales necesarias a un buen soldado (Gross, 2021).

4.1. Impacto de la biología sintética y de la inteligencia artificial en la revolución Bio

El desarrollo de la biología sintética, o *Syn-bio* como se la conoce en inglés, tendrá una importancia capital para el desarrollo de contramedidas médicas en su más amplio concepto, con el objetivo de minimizar o anular los riesgos y amenazas a los que se enfrentará el combatiente. Sin embargo, es fundamental tener en cuenta que podrá ser utilizada en programas químicos o biológicos por parte de actores estatales o no estatales. De ahí la importancia de la preparación para hacer frente a esas nuevas amenazas que el futuro puede depararnos (Aftergood, 2017).

Uno de los aspectos más importantes relacionado con las aplicaciones de IA en el ámbito de la Protección de la Fuerza, es y será la protección de los datos desde un punto de vista operativo, ya que obviando los aspectos éticos y legales relacionados con los derechos de los individuos sobre sus datos y la necesidad perentoria de anonimización de los mismos, los resultados de la aplicación de IA podrían ser manipulados con fines espurios alterando los algoritmos para generar información equivocada que llevara a adoptar por parte del comandante decisiones sesgadas. Por otro lado, no se puede olvidar que esa información, aún sin manipular, puede resultar clave para alcanzar el éxito operacional. De ahí que la ciberseguridad asociada a la aplicación de herramientas de IA para establecer relaciones entre datos a través del *big data* debe ser máxima.

En la actualidad resulta muy aventurado predecir cuál será el impacto de la IA, sola o en conjunción con otros desarrollos tecnológicos, en el ámbito de la seguridad y de la defensa, ya que es ahora cuando se están planteando cuáles son los riesgos derivados de ella, más allá de los generados por las armas autónomas (*International Committee of the Red Cross*, 2021), de ahí que resulte vital, al igual que lo que sucedió con la Conferencia de Asilomar con el desarrollo e implantación de códigos de conducta relacionados con la investigación en la recombinación del ADN, establecer las herramientas

de verificación y control efectivas frente a este tipo de iniciativas para impedir una mala aplicación de la IA con fines ilícitos (*United Nations for Disarmament Affairs*, 2023).

5. Reducción de riesgos y amenazas generados por la revolución Bio

A lo largo del texto se ha hecho hincapié en los efectos perjudiciales para la Protección de la Fuerza derivados de la aplicación torticera de los desarrollos asociados a la Revolución Bio en la que estamos inmersos, pudiéndose extractar como lecciones identificadas que no aprendidas:

- La necesidad de potenciación de la bioseguridad de las instalaciones, pero también de los programas de investigación que se lleven a cabo. Para ello, resulta fundamental establecer un control nacional e internacional de las secuencias de genes susceptibles de ser empleadas en programas biológicos, sin olvidar la necesidad perentoria de incrementar las medidas de biocustodia de agentes biológicos. Esto es así porque en función de las misiones asignadas pudiéramos estar desplegados en áreas donde pudiera producirse un accidente en una instalación donde se manejan agentes biológicos. Y en un escenario más peligroso podría producirse una diseminación intencionada.
- Potenciar la cultura de responsabilidad en los sectores implicados, en los productos obtenidos y en las técnicas utilizadas, más ahora que con la simplificación de las técnicas y el desarrollo de filosofías asociadas al transhumanismo o al movimiento *biohacking* ha aumentado el peligro asociado al manejo de agentes biológicos, sin las necesarias medidas de protección.
- Potenciar la capacidad de investigación, desarrollo y producción de contramedidas sanitarias y no sanitarias en un entorno de cooperación cívico-militar.
- Potenciar las capacidades sanitarias militares para poder dar respuesta a las necesidades derivadas de un incidente de diseminación de agentes químicos o biológicos en cualquier circunstancia.
- Mantener un estado de sospecha constante frente a la posibilidad de sufrir un incidente biológico a merced del establecimiento de un sistema de vigilancia epidemiológica en tiempo real. Esto permitirá activar el sistema de respuesta temprana y minimizar las consecuencias del incidente.

6. Conclusiones

La revolución Bio tendrá un impacto claro en el entorno de seguridad y defensa. Razón por la que tenemos que realizar un esfuerzo de preparación para hacer frente a los retos y desafíos futuros.

La práctica totalidad de las medidas de prevención frente a las amenazas deben adoptarse en el nivel político, pero también en el educativo, ya que hay que establecer los controles en la investigación, fundamentalmente en las de uso dual.

Es necesario promover la universalidad sin reservas de la CABT y cuantas iniciativas se establezcan para reducir el peligro de la proliferación a efectos de desarrollar una herramienta de verificación.

Apoyar la mejora de los programas nacionales e internacionales destinados a prevenir y combatir la propagación de enfermedades infecciosas, así como aquellos dedicados al desarrollo de contramedidas sanitarias.

Potenciar las capacidades sanitarias para dar respuesta a los retos a los que nos podamos enfrentar en un futuro no tan lejano.

7. Bibliografía

Aftergood, S. (2017). *Synthetic Biology and the Chem/Bio Threat*. Federation of Atomic Scientist. Disponible en: https://fas.org/publication/dod-cbw-2017/

Almosara, J. O. (2010). *Biotechnology: Genetically Engineered Pathogens*. Defense Technical Information Center. Disponible en: https://apps.dtic.mil/sti/tr/pdf/ADA556597.pdf

Blumenthal, M. *et al.* (2021). *Technological Approaches to Human Performance Enhancement*. Santa Mónica, RAND Corporation. Disponible en: https://www.rand.org/pubs/research_reports/RRA1482-2.html

Bokan, S. (2005). The toxicology of bioregulators as potential agents of bioterrorism. *Arh Hig Rada Toksikol*. 56, pp. 205-211.

Bollero, D. (2018). Las modificaciones genéticas y el temor a la eugenesia. *Público*. Disponible en: https://www.publico.es/ciencias/modificaciones-geneticas-temor-eugenesia.html

Centers for Disease Control and Prevention and Animal and Plant Health Inspection Service. (2023). *Select Agents and Toxins List*. Federal Select Agent Program. Disponible en: https://www.selectagents.gov/sat/list.htm?CDC_AA_refVal=https%3A%2F%2Fwww.selectagents.gov-%2FSelectAgentsandToxinsList.html

Charvet, B. *et al.* (2023). SARS-CoV-2 awakens ancient retroviral genes and the expression of proinflammatory HERV-W envelope protein in COVID-19 patients. *iScience*. 26. DOI: 10.1016/j.isci.2023.106604

Committe on Armed Services House of Representatives. (1999). New World Coming: American security in the 21st Century. En: *C. O. Representatives,*

The Phase One Report of the United States Commission on National Security/21 ST Century, p. 70.

Departamento de Seguridad Nacional. (2021). *Estrategia de Seguridad Nacional 2021. Un proyecto compartido.* Disponible en: https://www.dsn.gob.es/sites/dsn/files/ESN2021%20Accesible_1.pdf

Dilanian, K. (2020). China has done human testing to create biologically enhanced super soldiers, says top U.S. official. *NBC News*. Disponible en: https://www.nbcnews.com/politics/national-security/china-has-done-human-testing-create-biologically-enhanced-super-soldiers-n1249914

Du Cluzel, F. (2020). Cognitive Warfare. *Innovation Hub.* Disponible en: https://www.innovationhub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf

Edwards, C. (2022). MURDER-BOT Killer AI invented 40 000 'lethal chemical weapons' in just six hours – leaving scientists terrified. *The U.S. Sun*. Disponible en: https://www.the-sun.com/tech/4925922/killer-ai-invents-lethal-chemical-weapons/

ETC Group. (2017). Los archivos de los impulsores genéticos. *Gene Drive Files*. ETC Group. Disponible en: https://www.etcgroup.org/es/content/los-archivos-de-los-impulsores-geneticos

Evers, M. y Chui, M. (2021). The Promise and Peril of the Bio-Revolution. *Project Syndicate*. Disponible en: https://www.project-syndicate.org/commentary/biological-innovation-promise-and-perils-by-matthias-evers-and-michael-chui-2021-01/spanish?barrier=accesspaylog

Evers, M. *et al.* (2023). *Europe's Bio Revolution: Biological innovations for complex problems.* McKinsey&Company. Disponible en: https://www.mckinsey.com/industries/life-sciences/our-insights/europes-bio-revolution-biological-innovations-for-complex-problems#/

Farkas, C. B. *et al.* (2023). Analysis of the Virus SARS-CoV-2 as a Potential Bioweapon in Light of International Literature. *Mil Med.* 188, pp. 531-540. DOI: 10.1093/milmed/usac123

Fouchier, R. A. (2015). Studies on influenza virus transmission between ferrets: The public health risks revisited. *MBio.* 6. DOI: 10.1128/mBio.02560-14

Giersch, K., Dandri, M. (2015). Hepatitis B and Delta Virus: Advances on Studies about Interactions between the Two Viruses and the Infected Hepatocyte. *Journal of Clinical and Translational Hepatology.* 3, pp. 220-229. DOI: 10.14218/JCTH.2015.00018

Gross, M. L. (2021). Warfighter Enhancement: Research and Technology. *Military Medical Ethics in Contemporary Armed Conflict: Mobilizing*

Medicine in the Pursuit of Just War, pp. 181-260. New York, Oxford University Press. DOI: 10.1093/med/9780190694944.003.0010

Gross, T. (2019). The CIA's Secret Quest For Mind Control: Torture, LSD And A 'Poisoner In Chief'. *Npr.* Disponible en: https://www.npr.org/2019/09/09/758989641/the-cias-secret-quest-for-mind-control-torture-lsd-and-a-poisoner-in-chief

Henn, V. y Imken, M. (2022). *Organismos con impulsores genéticos: Una nueva dimensión en la Ingeniería Genética. Aplicaciones, riesgos y normativa.* Save Our Seeds/Foundation for Future Farming. Disponible en: https://www.ecologistasenaccion.org/wp-content/uploads/2022/09/informe-impulsores-geneticos.pdf

Herfst, S. *et al.* (2012). Airborne Transmission of Influenza A/H5N1 Virus Between Ferrets. *Science*. 336, pp. 1534-1541. DOI: 10.1126/science.1213362

Hessel, A., *et al.* (2012). Hacking the President's DNA. *The Atlantic.* Disponible en: https://www.theatlantic.com/magazine/archive/2012/11/hacking-the-presidents-dna/309147/

Hidalgo García, M. (2016). *La revisión de la aplicación del comité 1540. Documento Informativo 06/16*. Instituto Español de Estudios Estratégicos. Disponible en: https://www.ieee.es/Galerias/fichero/docs_informativos/2016/DIEEEI06-2016_Resolucion_1540_MMHG.pdf

Hunt, K. (2023). Cómo avanza la edición genética humana tras el escándalo de las bebés CRISPR. *CNN en Español.* Disponible en: https://cnnespanol.cnn.com/2023/03/13/como-avanza-edicion-genetica-humana-escandalo-bebes-crispr-trax/

International Committee of the Red Cross. (2021). ICRC Position on Autonomous Weapon Systems. Disponible en: https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems

Jackson, R. J. *et al.* (2001). Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. *Journal of Virology.* 75, pp. 1.205-1.210. DOI: 10.1128/JVI.75.3.1205-1210.2001

Kagan, E. (2006). Bioregulators as prototypic nontraditional threat agents. *Clinics in Laboratory Medicine.* 26, pp. 421-423. DOI: 10.1016/j.cll.2006.03.007

Kania, E. B., Vorndick, W. (2019). Weaponizing Biotech: How China's Military Is Preparing for a 'New Domain of Warfare'. *Defense One.* Disponible en: https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/

Kupferschimdt, K. (2017). How Canadian researchers reconstituted an extinct poxvirus for $100,000 using mail-order DNA. *Science*. Disponible en: https://www.science.org/content/article/how-canadian-researchers-reconstituted-extinct-poxvirus-100000-using-mail-order-dna

Lederberg, J. (1968a). DNA splicing Will fear rob us of its benefits?. *The Washington Post*. Disponible en: https://profiles.nlm.nih.gov/spotlight/bb/catalog/nlm:nlmuid-101584906X1164-doc

—(1968b). Hailing ORNL Example of «Genetic Engineering». *The Oak Ridger.* Disponible en: https://collections.nlm.nih.gov/catalog/nlm:nlmuid-101584906X1168-doc

Lee, M. *et al.* (2020). *The Internet of Bodies: Opportunities, Risks, and Governance*. Santa Mónica, RAND Corporation. Disponible en: https://www.rand.org/pubs/research_reports/RR3226.html

Locatelli, F. *et al.* (2022). Betibeglogene Autotemcel Gene Therapy for Non–β0/β0 Genotype β-Thalassemia. *New England Journal of Medicine*. 386, pp. 415-427. DOI: 10.1056/NEJMoa2113206

López Baroni, M. J. (2015). Implicaciones éticas de las investigaciones con virus: el Principio de Colaboración Global. *Revista de Bioética y Derecho*. 34, pp. 37-52. Disponible en: https://scielo.isciii.es/pdf/bioetica/n34/articulo4.pdf

Masaki, I. *et al.* (2012). Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. *Nature*. 486, pp. 420-428.

Mayfield, M. (2020). *China Pursuing 'Aggressive' Biotechnology Strategy.* National Defense. Disponible en: https://www.cnas.org/publications/commentary/weaponizing-biotech-how-chinas-military-is-preparing-for-a-new-domain-of-warfare

Mendz, G. y Cook, M. (2021). Transhumanist Genetic Enhancement: Creation of a 'New Man' Through Technological Innovation. *New Bioeth.* 27, pp. 105-106. DOI: 10.1080/20502877.2021.1917228

Merck, G. W. (1945). *Report to the Secretary of War by Mr. George W. Merck, Special consultant for biological warfare*. National Academy of Sciences. Disponible en: http://www.nasonline.org/about-nas/history/archives/collections/organized-collections/1945merckreport.pdf

National Academies of Sciences, Engineering, and Medicine. (2018). *Biodefense in the Age of Synthetic Biology.* Washington, DC, The National Academies Press. DOI: 10.17226/24890

National Security Technology Acceleration. (2023). *Biotecnology on the Battlefield*. NSTXL. Disponible en: https://nstxl.org/biotechnology-on-the-battlefield/

Needham, K. y Baldwin, C. (2021). China's gene giant harvests data from millions of women. *Taipei Times*. Disponible en: https://www.taipeitimes.com/News/feat/archives/2021/07/10/2003760597

Nicholson, P. J. *et al.* (2015). *Cognitive enhancing drugs and the workplace*. British Medical Association. Disponible en: https://www.bma.org.uk/media/1068/bma_cognitive_enhancing_drugs_and_the_workplace_oct_2019.pdf

Nieuwenhuizen, M. S. y Lagenberg, J. P. (2008). *Biotechnologies for Assessment of Toxic Hazards in Operational Environments. RTO Technical Report - TR-HFM-057*. Research and Technology Organisation of NATO. DOI: 10.14339/RTO-TR-HFM-057

Noble, S. M. *et al.* (2022). The Fifth Industrial Revolution: how harmonius human-machine collaboration is triggering a retail and service [R]evolution. *Journal of Retailing*. 98, pp. 199-208. DOI: 10.1016/j.jrati.2022.04.003

Pagani, I. *et al.* (2023). Origin and evolution of SARS-CoV-2. *The European Physical Journal Plus*. 138, pp. 157-163. DOI: 10.1140/epjp/s13360-023-03719-6

Petro, J. B. *et al.* (2003). Biotechnology: impact on biological warfare and biodefense. *Biosecur Bioterror*. 1, pp. 161-168. DOI: 10.1089/153871303769201815

Prados de la Escosura, L. (2021). Augmented human development in the age of globalization. *The Economic History review*. 74, pp. 946-975. DOI: 10.1111/ehr.13064

Price, L. B. *et al.* (2003). In vitro selection and characterization of Bacillus anthracis mutants with high-level resistance to ciprofloxacin. *Antimicrobial Agents Chemother*. 47, pp. 2.362-2.365.

Przekora, A. (2020). A Concise Review on Tissue Engineered Artificial Skin Grafts for Chronic Wound Treatment: Can We Reconstruct Functional Skin Tissue In Vitro? *Cells*. 9, p. 1.622. DOI: 10.3390/cells9071622

Requena, T. y Velasco, M. (2021). Microbioma humano en la salud y la enfermedad. *Revista Clínica Española*. 221, pp. 233-240. DOI: 10.1016/j.rce.2019.07.004

Reuters. (2022). Macron no aceptó la prueba de PCR en Rusia para que Putin «no tuviera su ADN». *ABC* [en línea]. Disponible en: https://www.

abc.es/internacional/abci-razones-putin-mantuvo-distancia-macron-durante-encuentro-202202102128_noticia.html

Ricci, G. (2020). Pharmacological Human Enhancement: An Overview of the Looming Bioethical and Regulatory Challenges. *Front Psychiatry.* 11. DOI: 10.3389/fpsyt.2020.00053

Rigaud, N. (2008). *The Organisation for Economic Co-operation and Development. Biotechnology: Ethical and social debates*. OECD. Disponible en: https://www.oecd.org/futures/long-termtechnologicalsocietalchallenges/40926844.pdf

Rimmington, A. (2021). Genesis: The Creation of Biopreparat. En: *R. A, The Soviet Union's Invisible Weapons of Mass Destruction*. Palgrave McMillan, pp. 49-72. DOI: 10.1007/978-3-030-82882-0_4

Rosenzweig, P. (2022). Artificial Intelligence and Chemical and Biological Weapons. *Lawfare*. Disponible en: https://www.lawfaremedia.org/article/artificial-intelligence-and-chemical-and-biological-weapons

Rothman, A. *et al*. (2023). How Synthetic Biology Can Make a Materials Difference. *Boston Consulting Group.* Disponible en: https://www.bcg.com/publications/2023/how-synthetic-biology-materials-can-make-a-difference

Alitskii, A. I. y Salitskaya, E. A. (2022). China on the Way to Global Technology Leadership. *Herald of the Russian Academy of Sciences.* 92, pp. 262-267. DOI: 10.1134/S1019331622030042

Sánchez, G. B. (2018). Las primeras cinco revoluciones industriales. *Cienciorama*. Universidad Autónoma de México. Disponible en: http://www.cienciorama.unam.mx/a/pdf/585_cienciorama.pdf

Science and Technology Organization. (2021). *Biotechnology, Human Enhancement and Human Augmentation: A Way Ahead for Research and Policy (STO-TR-HFM-ST-335-A).* DOI: 10.14339/STO-TR-HFM-ST-335-A

Sears, R. G. *et al*. (2023). Engineered gamma radiation phytosensors for environmental monitoring. *Plant Biotechnology Journal.* 21, pp. 1.745-1.756. DOI: 10.1111/pbi.14072

Sebastián-Domingo, J. J. y Sánchez-Sánchez, C. (2018). De la flora intestinal al microbioma. *Revista española de enfermedades digestivas*. 110, pp. 51-56. DOI: https://dx.doi.org/10.17235/reed.2017.4947/2017

Sebelius, K. (2011). Why We Still Need Smallpox. *The New York Times*. Disponible en: https://www.nytimes.com/2011/04/26/opinion/26iht-edsebelius26.html

Sentís, C. (2002). Retrovirus endógenos humanos: Significado biológico e implicaciones evolutivas. *Arbor.* 172, pp. 135-166. DOI: 10.3989/arbor.2002.i677.1073

Sharma, A. *et al.* (2020). Next generation agents (synthetic agents): Emerging threats and challenges in detection, protection, and decontamination. En: Pachauri, S. F. (ed.). *Handbook on Biological Warfare Preparedness*. Academic Press, pp. 217-256. DOI: https://doi.org/10.1016/B978-0-12-812026-2.00012-8

The Lancet Microbe. (2022). Searching for SARS-CoV-2 origins: confidence versus evidence. *The Lancet Microbe*. 4, e471. DOI: 10.1016/S2666-5247(23)00074-5

Tucker, P. (2020). AI Is Reshaping the US Approach to Gray-Zone Ops. *Defense One*. Disponible en: https://www.defenseone.com/technology/2020/12/ai-reshaping-us-approach-gray-zone-ops/170621/

UNESCO. (2021). *Informe sobre la ciencia 2021*. Disponible en: https://www.unesco.org/reports/science/2021/es/china

United Nations for Disarmament Affairs. (2023). *Scientific and Technological Developments: Benefits and Risks for the Biological Weapons convention: Conference Report*. United Nations Organization. Disponible en: https://front.un-arm.org/wp-content/uploads/2023/08/Conference-report_ST-developments.pdf

Urbina, F., *et al.* (2022). Dual use of artificial-intelligence-powered drug discovery. *Natural Machine Intelligence*. 4, pp. 189-191. DOI: 10.1038/s42256-022-00465-9

Vicki, L. A. *et al.* (2006). Bacillus anthracis virulent plasmid pX02 genes found in large plasmids of two other Bacillus species. *Journal of Clinical Microbiology*. 44, pp. 2.367-2.377. DOI: 10.1128/JCM.00154-06

Warmbrod, K. L. *et al.* (2021). COVID-19 y los debates sobre la ganancia de función. *EMBO Reports*. 22, e53739. DOI: 10.15252/embr.202153739

Wickiser, J. *et al.* (2020). Engineered Pathogens and Unnatural Biological Weapons: The Future Threat of Synthetic Biology. *CTC Sentinel*. 13, pp. 1-7.

Woo, P. C. *et al.* (2009). Coronavirus Diversity, Phylogeny and Interspecies Jumping. *Experimental Biology and Medicine*. 234. pp. 1.117-1.127. DOI: 10.3181/0903-MR-94

Yanes, J. (2023). ¿Debe prohibirse aumentar la agresividad de los virus? *OpenMind BBVA*. Disponible en: https://www.bbvaopenmind.com/ciencia/apuntes-cientificos/debe-prohibirse-aumentar-la-agresividad-de-los-virus/

Capítulo 4

Dispositivos móviles personales: riesgos multidominio en la palma de la mano

José Ángel Tortosa Delfa

Resumen

Los dispositivos móviles personales forman parte intrínseca del ser humano desde hace años. En el entorno operativo previsible, vamos a asistir a una evolución en esa relación, pues su conectividad mejorada, su capacidad de procesamiento y la miríada de sensores miniaturizados de que dispondrán los auparán a la cúspide de los dispositivos electrónicos. Se convertirán en el principal medio por el que el ser humano se conecte con su yo digital y por el que reciban la información del mundo que les rodea. Esta situación privilegiada los hace, a su vez, una herramienta multidominio capaz de generar amenazas físicas, virtuales y cognitivas. Asegurar la Protección de la Fuerza en un entorno sobresaturado de estos dispositivos, no solo dentro de la Fuerza, sino también a su alrededor, se torna en una actividad que debe combinar la resiliencia de las redes, el refuerzo de las capacidades de información, el control proactivo y la agilidad de empleo para asegurar la libertad de acción del mando. La solución para gestionar este riesgo no vendrá de la prohibición de empleo de los dispositivos personales, sino de entender cómo integrarlos en la Fuerza.

Palabras clave

Protección de la Fuerza, Multidominio, Dispositivos móviles personales, PED.

Personal mobile devices: multi-domain risks in the palm of your hand

Abstract

Portable electronic devices have been an integral part of human life for years. In the foreseeable operational environment, we will witness an evolution in this relationship, as their enhanced connectivity, processing power, and the myriad of miniaturized sensors they will possess will propel them to the pinnacle of electronic devices. They will become the primary means by which humans connect with their digital selves and receive information about the world around them. This privileged position also makes them a multidomain tool, capable of generating physical, virtual, and cognitive threats. Ensuring Force Protection in an environment saturated with these devices, not only within the Force but also in its vicinity, becomes an activity that must combine network resilience, enhanced information capabilities, proactive control, and agility in its use to ensure the commander's freedom of action. The solution to managing this risk will not come from prohibiting the use of personal devices but from understanding how to integrate them into the Force.

Keywords

Force Protection, Multidomain, Portable electronic devices, PED.

1. Introducción

El caballo de Troya

«O en esa armazón de madera hay gente oculta, o se ha fabricado en daño de nuestros muros, con objeto de explorar nuestras moradas y dominar desde su altura la ciudad, o algún otro engaño esconde. ¡Troyanos, no creáis en el caballo!» (Virgilio, s. f.).

El caballo que propició la caída de Troya cruzó los muros de la ciudad gracias al esfuerzo de sus propios habitantes. Los troyanos vieron un presente donde debían ver un peligro y cuando se dieron cuenta de lo que en realidad sucedía, ya era demasiado tarde. Esta leyenda épica, universal e inmortal, guarda una lección que en pleno siglo XXI sigue estando tan vigente como en los tiempos de Virgilio: los dispositivos móviles personales son un regalo con el que podemos meter al enemigo en casa.

Aunque los primeros teléfonos móviles aparecieron en la década de los setenta, la verdadera revolución de los dispositivos personales no llegó hasta la aparición de los teléfonos inteligentes, veinte años después y, sobre todo, con el despliegue de las redes de comunicación móvil 3G. Desde de ese momento, la carrera por aumentar la velocidad de transferencia de datos y la potencia de estos dispositivos han llevado a la sociedad a adoptarlos como principal medio de comunicación, pasando a formar parte integral de la actividad cotidiana del ser humano.

La guerra que se desató tras la invasión de Ucrania por parte de Rusia en febrero de 2022 ha puesto de manifiesto cómo un conflicto convencional-tradicional puede adaptarse a las últimas tecnologías y, a su vez, adaptarlas para su empleo en combate. La irrupción masiva de los drones en el campo de batalla, el mando y control mediante dispositivos COTS[1], la saturación informativa, la desinformación o el empleo del ciberespacio como espacio de confrontación son solo algunos de los ejemplos que reflejan la naturaleza cambiante de la guerra. Todos estos ejemplos, sin embargo, tienen un denominador común: los dispositivos móviles personales.

Los dispositivos electrónicos móviles de uso personal (PED[2]), que a efectos de este trabajo se definen como sistemas electrónicos y de información portátiles con capacidades conectivas, se han convertido en la argamasa que une a las personas, hiperconectando al individuo con la sociedad global. Para poner en perspectiva la importancia que tienen para el ser humano, basta con presentar algunas estadísticas de uso:

1 Del inglés *Commercial-off-the-shelf*, se refiere a componentes o dispositivos comercializados en el mercado general que pueden adquirirse sin ningún tipo de restricción.

2 Del inglés *Portable Electronic Devices*.

- El 96 % de la población mundial entre 16 y 64 años dispone de teléfono inteligente, que la mayor parte del tiempo se encuentra a su inmediato alcance.
- El tiempo medio que pasamos en internet supera las seis horas diarias, de las que más de dos horas y media las dedicamos a las redes sociales.
- Dedicamos cinco veces más tiempo a navegar por internet desde dispositivos móviles que desde dispositivos de sobremesa (Kemp, 2023).

Frente a un declive en el uso de los grandes dispositivos electrónicos, ciertos PED, relacionados con la monitorización del ser humano e incluso con el acceso a la realidad virtual, empiezan a ser adoptados de manera paulatina y sus índices de crecimiento apuntan a un uso generalizado en el entorno operativo futuro.

Las comunicaciones móviles han pasado a ser una obviedad para las sociedades avanzadas. Del mismo modo que no ponemos en duda la disponibilidad permanente de electricidad para garantizar nuestro bienestar en el día a día, damos por supuesto que contamos con un objeto portátil a nuestro alcance que nos mantiene perpetuamente hiperconectados, con capacidad inmediata de acceder al «infoverso» que proporciona internet y captar la realidad que nos rodea. En 2040 se estima que existirán casi cien mil millones de dispositivos interconectados (Ministerio de Defensa, 2021: 20) que, de una u otra manera, tendrán relación con todos los ámbitos en los que operarán las Fuerzas Armadas: los ámbitos físicos tradicionales (terrestre, marítimo y aeroespacial), el ciberespacio y el ámbito cognitivo.

La relevancia de los PED en los conflictos no es nueva; su uso se asocia desde hace años al combate asimétrico y las actividades de insurgencia. Su omnipresente amenaza a las fuerzas desplegadas en entornos de lucha contra el terrorismo, como Afganistán, propició incluso cambios en la doctrina que regula la Protección de la Fuerza (PF).

Sin embargo, el desarrollo de las redes 5G, la evolución tecnológica y la miniaturización de estos aparatos hace que, en el futuro entorno operativo, la presencia masiva de PED, tanto alrededor de la fuerza como en su seno, suponga un nuevo desafío para la PF que será necesario abordar de forma proactiva, minimizando las amenazas que puedan limitar la libertad de acción y la operatividad. Estos dispositivos van a alcanzar capacidades cuasi-convencionales y generar efectos físicos, virtuales y cognitivos muy significativos, lo que los habilitará, de hecho, como herramienta multidominio.

1.1. Alcance

Este capítulo analiza el impacto que tiene el empleo de los PED para las operaciones de las Fuerzas Armadas y la relación que existe entre estos dispositivos

y la PF, desde un punto de vista prospectivo. Para ello, se valoran aquellas tendencias tecnológicas y sociales de especial repercusión en el entorno operativo previsible, partiendo de la situación actual, marcada muy significativamente por la invasión rusa de Ucrania en 2022. Este conflicto, por la presencia de capacidades convencionales tecnológicamente avanzadas y la experimentación que se está haciendo de la combinación de tecnologías estándar con sistemas militares, resulta paradigmático para valorar cómo se normalizará el papel de los PED en el espacio de las operaciones futuro. Al ser un trabajo prospectivo, no se ofrecen soluciones cerradas, sino que se tratan de identificar factores clave para adaptar la Fuerza al entorno operativo previsible.

El estudio tiene en cuenta la amalgama de PED de uso militar y civil/privado que existirán en el campo de batalla, aunque el foco se dedica a estos últimos. La principal vulnerabilidad que se deriva del uso de los PED se relaciona con la profusión de aparatos disponibles dentro y alrededor de nuestras Fuerzas, cuyo origen e incluso capacidades serán desconocidos, con la dificultad que tendrá limitar o controlar su uso, los porten combatientes o no.

2. Futuro de los dispositivos móviles en el entorno operativo

Los PED pueden ser aparatos de naturaleza muy variada. En el entorno operativo actual es fácil identificar los PED con nuestros habituales teléfonos móviles, los sistemas de captación y grabación multimedia, los aparatos de localización o los monitores de actividad. También se pueden entender como tales escáneres, sensores de radiofrecuencia o biológicos (siempre en relación con el uso personal).

Las dos principales características de los PED, su capacidad de interactuar con otros sistemas de información y su portabilidad, van a acentuarse en los próximos años. El futuro de la computación y la comunicación radica en los dispositivos móviles. Su tamaño, creciente capacidad de procesamiento y flexibilidad los hacen dispositivos ideales para la movilidad e inmediatez que demanda la sociedad. En el entorno operativo futuro, podemos esperar una adopción generalizada del Internet de las Cosas, los dispositivos de realidad virtual y realidad aumentada, junto con el empleo de la inteligencia artificial (IA) en la práctica totalidad de los dispositivos electrónicos, todo ello unido a una mejora en su capacidad de computación, miniaturización y autonomía.

Los teléfonos móviles evolucionarán hacia dispositivos de comunicaciones «siempre encendidos-siempre conectados» gobernados por la IA, reduciendo así la carga de trabajo del ser humano y automatizando el intercambio de información. La sobresaturación de constelaciones de comunicaciones en el espacio y la disponibilidad de comunicaciones terrestres resilientes van a hacer muy difícil limitar la conectividad de estos dispositivos, incluso en áreas afectadas por acciones de guerra electrónica.

Los dispositivos que se visten o *wearables*, como pueden ser los mencionados dispositivos de realidad aumentada, los sensores biométricos o el camuflaje personal activo van a pasar a formar parte del material disponible de forma habitual. Esto dará lugar a una «sensorización» del ser humano que se podrá utilizar para aplicaciones como la medición del comportamiento, la monitorización médica, la seguridad biométrica y la ocultación.

Junto a estas tendencias, se prevé una incorporación paulatina de tecnologías menos desarrolladas hasta el momento, como las nubes portátiles, la integración hombre-máquina, la implantación de nanosensores, los sistemas de posicionamiento inercial miniaturizado o el diseño y fabricación instantánea de aparatos electrónicos *ad hoc* (*National Intelligence Council*, 2021).

En el entorno operativo previsible, existen conceptos como los enjambres de drones y la «guerra mosaico» o distribuida que se pueden beneficiar de la alta presencia de PED. La «guerra mosaico» tratará de minimizar el riesgo que, para una fuerza, supone contar con sistemas y plataformas de alto valor (militar y económico) en cantidades limitadas. La combinación de geolocalización, conocimiento de la situación y comunicaciones instantáneas puede hacer innecesario contar con estos grandes sistemas de armas en favor de una combinación de sistemas flexibles, pequeños y baratos (Jensen y Paschkewitz, 2019). Estas características se adaptan a la perfección a los PED, por lo que no es descartable que nuestra Fuerza se enfrente en el futuro a sistemas mosaico generados mediante una combinación de múltiples dispositivos personales conectados a sistemas de armas.

A veinte años vista, cuatro características van a definir los desarrollos tecnológicos alrededor del combate: inteligencia, conectividad, descentralización y digitalización (Reding *et al.,* 2023: 10-12). Estas características, adaptadas a los dispositivos personales, los convertirán en aparatos con una avanzada autonomía a la hora de decir qué datos recopilar y transmitir, capaces de conformarse en centros de datos y de computación; con una conectividad mayor que contribuirá a la transmisión casi instantánea de grandes volúmenes de información; preparados para conformarse en partes de macrosistemas; y aptos para acceder a realidades aumentadas o entornos sintéticos inmersivos con una alta capacidad de interacción.

3. Los PED y la Protección de la Fuerza

La Protección de la Fuerza, según la doctrina conjunta de las FAS.

> «[…] engloba aquellas actividades que tienen como objeto minimizar la vulnerabilidad del personal, equipo, material, instalaciones, información, operaciones y actividades de la Fuerza y de los elementos no militares que apoyan, acompañan o están

> bajo responsabilidad de la Fuerza, frente a las acciones adversarias, propias, y frente a los riesgos sanitarios, naturales, tecnológicos y accidentes» (Estado Mayor de la Defensa, 2019: 3).

La PF trata de gestionar riesgos para preservar nuestra libertad de acción y lo hace estableciendo medidas encaminadas a contrarrestar o mitigar las amenazas, bien sean estas procedentes del adversario o presentes en el entorno.

Las características transversales de los PED suponen una amenaza para una gran parte de las áreas de aplicación de la PF, como son la seguridad de la información (incluyendo la seguridad de los sistemas de información y telecomunicaciones), la seguridad física, la seguridad en las operaciones[3] (OPSEC), la seguridad de la propia organización (frente a la desinformación y descrédito) o la protección contra amenazas no convencionales.

Las medidas necesarias para gestionar el riesgo procedente de los PED pueden ser muy diferentes en función de las características de los ámbitos en los que opere la Fuerza:

- Ámbito terrestre: este ámbito de operación, donde se producen la mayoría de las interacciones humanas, es en el que existirá una mayor presencia de PED en y alrededor de la Fuerza, en el que será más difícil garantizar la OPSEC. En el futuro, esta saturación de dispositivos se va a acentuar, favoreciendo acciones permanentes de monitorización y *targeting*, aumentando el número de amenazas a la infraestructura vital para la misión.
- Ámbito marítimo: la amenaza que suponen los PED en el entorno marítimo no es muy diferente de otras amenazas ya existentes; los puntos críticos estarán principalmente relacionados con las zonas de convergencia entre este ámbito y el terrestre, como la navegación por pasos obligados o las operaciones anfibias. Además, la naturaleza más aislada de este ámbito lo hace especialmente susceptible a los riesgos que comporta la existencia de PED no regulados dentro de las unidades que operan en él, mediante la combinación de acciones en los ámbitos ciberespacial y cognitivo.
- Ámbito aeroespacial: al igual que sucede en el ámbito marítimo, las zonas de convergencia entre este ámbito y el terrestre, como los aeródromos o el límite inferior del espacio aéreo, son críticas. Uno de los usos de los PED que más va a aumentar en zonas de conflicto es el control de

[3] La seguridad en las operaciones «establece medidas destinadas a proteger los Elementos Esenciales de Información Propia contra las acciones de obtención de información del adversario y de las filtraciones no deliberadas o autorizadas de las fuerzas propias» (Estado Mayor de la Defensa, 2019: 12).

drones. Los PED van a contribuir a generar un espacio saturado de sistemas fungibles o de fácil reposición que incrementarán los riesgos de las aeronaves que operen en él. Por otro lado, el espacio ultraterrestre se utilizará en profusión para habilitar los PED: las comunicaciones satelitales a escala global harán prácticamente imposible limitar la conectividad regional o local. La actual privatización de los sistemas de comunicaciones se va a extender y supondrá la presencia de sistemas satelitales en manos de corporaciones privadas con objetivos propios.

En septiembre de 2023, el magnate de las finanzas Elon Musk reconoció haber denegado el uso de su servicio de internet satelital Starlink, de SpaceX, al Ejército ucraniano. Con ello, evitaba que Starlink se utilizase para ejecutar un ataque dron contra la flota rusa y, en las propias palabras de Musk, impedía que «SpaceX se convirtiera en cómplice explícito de un acto de guerra y escalada del conflicto» (Klim, 2023). Esta actuación pone de relieve el poder que pueden tener las corporaciones para decidir sobre cuestiones operativas, si no se establece un adecuado marco de colaboración y empleo.

- Ámbito ciberespacial: a medio plazo, se espera un incremento de avances tecnológicos adversos o disruptivos que derivarán en riesgos en el ciberespacio (Ministerio de Defensa, 2021: 30). La mayor dependencia que existirá del ciberespacio por parte de la sociedad, junto a la creciente necesidad de movilidad, tornarán a los PED en el principal punto de acceso a un universo digital sin el que no podremos desarrollar nuestra actividad cotidiana. Por ello, aumentarán las vulnerabilidades relacionadas con el yo digital. La mejora prevista en los sistemas de seguridad y encriptación de los dispositivos traerá consigo un crecimiento en el número de riesgos asociados a la generación y análisis de datos sobre el comportamiento de las personas y la identidad digital. El desarrollo de metaversos virtuales contribuirá a desdibujar la línea que existe entre este ámbito y el cognitivo. En muchos casos las acciones cibernéticas perseguirán efectos duales virtual-cognitivo. Más allá, tecnologías embrionarias en la actualidad, como los interfaces hombre-máquina, podrían convertir al ser humano en objeto de ciberataques.
- Ámbito cognitivo: este ámbito de operación va a seguir cobrando importancia en el entorno operativo futuro. La guerra de Ucrania ha confirmado «los riesgos masivos a la seguridad en las operaciones que existen en sociedades interconectadas y la importancia de moldear el dominio de la información» (Colom-Piella, 2023: 10). La capacidad de procesamiento de los PED los hará capaces de generar campañas de influencia y desinformación automatizadas, basadas en inteligencia artificial y en el conocimiento cada vez más profundo de los procesos cerebrales. Los

wearables de realidad aumentada y virtual permitirán una inmersión sensorial mucho mayor del ser humano en la información que recibe, lo que lo hará mucho más susceptible a la manipulación.

3.1. BYOD

BYOD (del inglés *Bring your own device*) es una política de uso de dispositivos electrónicos que se ha extendido por todo tipo de organismos en los últimos años. Esta política permite que los empleados utilicen sus propios PED en el entorno de trabajo mediante conexión directa a los servidores de la organización, acceso remoto a los terminales corporativos, o a través de aplicaciones y capas de seguridad específicas instaladas en los propios dispositivos.

Esto supone numerosas ventajas respecto a la experiencia de uso de los empleados, al utilizar los dispositivos con los que se sienten más cómodos para trabajar, al tiempo que flexibiliza el entorno y los horarios en beneficio de la organización. Sin embargo, estas políticas deben venir acompañadas de medidas que mitiguen los riesgos derivados de ciberataques, dado que estos equipos personales se utilizan, a su vez, para acceder a todo tipo de redes y dominios.

Durante años, las FAS han hecho uso de esta política de forma limitada, permitiendo el acceso a información corporativa no clasificada. Esto ha supuesto normalizar el uso de PED privados en la organización (excepto en áreas clasificadas), lo que no hace, sino extender el empleo permanente de estos aparatos que se hace en el día a día de la sociedad y, por tanto, en parte intrínseca de la Fuerza. El combatiente del siglo XXI utiliza sus dispositivos de forma continua, creando dependencias que no se eliminan cuando despliega.

3.2. Los PED en los conflictos actuales

El uso de los PED, en especial los teléfonos móviles, esta transformando las actividades de mando y control, las comunicaciones y la inteligencia en los conflictos. Han transformado estas actividades, antes solo disponibles para los más sofisticados sistemas de armas, en colaborativas. Han proporcionado capacidades avanzadas a los escalones más bajos de la cadena de mando y a los civiles alrededor de la fuerza, mejorando su conocimiento de la situación y su agilidad. Sobre todo, han dotado de valor a la actuación anónima del individuo sobre el terreno.

Estas ventajas también han traído consigo vulnerabilidades que explotar por parte del enemigo. Por ello, la mayoría de los países cuentan con procedimientos estándar que, en general, limitan al máximo, cuando no prohíben,

el empleo de dispositivos personales en las operaciones. Esta limitación de uso en el frente se debe a una combinación de medidas de PF que incluyen la OPSEC, tratando de evitar que el adversario obtenga información de nuestras actividades, de seguridad de la información, para salvaguardar su confidencialidad, integridad y disponibilidad, así como de seguridad de la organización, frente a campañas de desinformación y propaganda.

Aun así, existen evidencias en los últimos conflictos de que esta prohibición no solo no se ha materializado, sino que en muchos casos los PED han pasado a ser herramientas esenciales para las tropas sobre el terreno. La guerra en Ucrania ha puesto de relieve una sistematización en el empleo de dispositivos móviles, en especial los teléfonos, para hacer la guerra. Lo que comenzó como un movimiento reactivo a la falta de medios, ha terminado generalizando el uso de PED como sensores y sistemas de mando y control, combinando en muchos casos *hardware* COTS con *software* específico (Horbyk, 2022).

La limitación de uso de los PED se trata de una medida difícil de implementar; los soldados terminan encontrando métodos para burlar las prohibiciones y hacen uso de sus móviles como herramienta de entretenimiento, comunicación y en apoyo a las operaciones. Por tanto, se establece un doble rasero en el empleo de los PED: limitaciones a nivel organizativo por parte de las FAS y autorización tácita de estos medios en entornos de conflicto.

3.3. Nativos digitales y los conflictos de larga duración

La prohibición o limitación de uso de los PED no tiene en cuenta dos de los factores principales que afectan a los combatientes del siglo XXI: la naturaleza digital y el tiempo. El término «nativo digital» apareció en 2001 para definir a las generaciones que han crecido en presencia de tecnologías digitales (Prensky, 2001) y que les ha dotado de características diferenciadas frente a generaciones anteriores. En general, el nativo digital es creativo, global, curioso, tiene iniciativa y capacidad multitarea. A su vez, presentan una independencia muy marcada en la búsqueda y creación de información, una clara dependencia de la sociedad virtual (entendida como las relaciones que se forman exclusivamente a través de redes sociales), una expectativa de inmediatez en todo lo que les rodea y un cierto recelo frente a intereses corporativos, que también puede extenderse a los intereses gubernamentales (García *et al.,* 2011). Estas últimas características pueden hacer al combatiente nativo de la era digital reacio a aceptar medidas restrictivas respecto a lo que, para él, es un elemento natural de su experiencia vital: el PED.

El tiempo es un factor difícil de cuantificar, pero que se relaciona directamente con una de las características del nativo digital mencionadas: la expectativa de inmediatez. Para esta generación, más que para las anteriores, el paso

del tiempo en los conflictos contribuye a minimizar los riesgos percibidos. En los primeros compases de una operación militar, las medidas de control funcionan mejor. A medida que se aumenta el tiempo de permanencia en zonas sujetas a los peligros inherentes al combate, el riesgo percibido por el uso de los PED privados se combina con otros riesgos y la conclusión puede ser que las ventajas que ofrece su empleo superan los riesgos asociados. A pesar de que existe una clara identificación de los PED como riesgo para la fuerza, también es cierto que se trata de uno de los primeros riesgos aceptados por el combatiente, por las ventajas que ofrece su uso.

3.4. La frontera que separa a combatiente y civil se difumina

Es importante recalcar que el empleo de PED desdibuja la línea que separa al combatiente del civil. El principio de distinción entre estos dos roles y la protección de los civiles, conforman la piedra de toque de la legislación que regula los conflictos armados. Sin embargo, cuando un civil utiliza su PED para obtener y enviar información de fuerzas militares, se participa activamente como sensor y, de facto, renunciando a su estatus protegido. Esto, que ya está sucediendo en Ucrania, «podría influir en futuros modelos de conducta, y después de un tiempo, convertirse en la norma global» (Olejnik, 2022).

Los riesgos para la PF que se experimentaron en escenarios de lucha antiterrorista y anti-insurgencia se amplifican en el combate del futuro. Toda persona presente en el entorno en el que operen fuerzas militares podrá actuar, potencialmente, como sensor y sistema de comunicaciones. Un civil podrá utilizar su PED de forma esporádica para enviar datos o automatizar la información que recopila de forma pasiva, alternando entre su condición de civil y su papel como combatiente en cuestión de minutos. Más aún, mediante acciones cibernéticas externas, cualquier individuo que porte un PED podría estar actuando contra las fuerzas propias involuntariamente.

La existencia de PED en escenarios de conflicto va a suponer un reto para la normativa que los regula; ante la duda del estatus de una persona, la Convención de Ginebra establece que se la debe tratar como a un civil. Esto afecta directamente a la PF, pues el número de potenciales amenazas se incrementará y las medidas de protección, sean activas o pasivas, deberán partir de la base de que todo elemento humano a su alrededor eleva el riesgo.

4. Amenazas y vulnerabilidades en las dimensiones de efectos

La nueva doctrina OTAN (2022) entiende las dimensiones de efectos como entornos conceptuales del espacio de las operaciones en los que se materializan las consecuencias y resultados (que pueden ser deseados o

indeseados) de las acciones que se llevan a cabo en los ámbitos de operación. Los efectos se contextualizan mediante tres dimensiones: la física, la virtual y la cognitiva. Una acción en cualquier ámbito de operación puede tener efectos en las tres dimensiones: así, por ejemplo, una acción ciberespacial para bloquear un puente levadizo podría tener efectos virtuales (anulación del sistema automático del puente), físicos (acumulación de vehículos), e incluso cognitivos (frustración de los ocupantes de esos vehículos). Al presentar los efectos que los PED pueden generar en estas tres dimensiones, se visualiza mejor su potencial como herramienta multidominio y se facilita la comprensión de las medidas necesarias para proteger a la Fuerza.

4.1. Dimensión física

Esta dimensión se relaciona con las consecuencias físicas de las acciones en las personas y el entorno en el que habitan, incluyendo los objetos físicos y las infraestructuras.

4.1.1. Localización y targeting

La capacidad de los PED de proporcionar información geoespacial esta instrumentalizándose desde hace años. Ya en 2018, los medios se hicieron eco de la filtración de los patrones de conducta de soldados estadounidenses y la localización de bases en Afganistán, gracias a dispositivos de monitorización de actividad.

Hoy en día, existen aplicaciones que aprovechan las capacidades colaborativas de los PED para obtener, transmitir y combinar información de geolocalización[4]. Estas aplicaciones proporcionan mapeado del terreno, herramientas de *targeting*, etiquetado, medición de distancias, incorporación de datos fotográficos, escaneo 3D, e incluso el enlace entre aparatos personales y sistemas militares... todo lo que un simple teléfono móvil puede aportar al combate hoy en día.

Se está desarrollando *software* muy variado que transforma el campo de batalla en un entorno colaborativo. Ejemplo de ello es el *Live Universal Awareness Map* (Disponible en: https://liveuamap.com/), que presenta información geoespacial y un agregador de noticias como aplicación web, combinando la recolección individual de miles de PED, comentarios en redes sociales y localización, para proporcionar una imagen general de

[4] La *suite Team Awareness Kit* (CivTAK/ATAK), desarrollada por el Air Force Research Laboratory estadounidense, se está utilizando con éxito en Ucrania. Para ello, solo es necesario instalar su *software*, disponible de forma gratuita en Google Play, en un teléfono móvil. Hasta el momento acumula más de cien mil descargas.

la situación en un conflicto. Tanto civiles como militares en zonas «calientes» actúan como pequeñas células de inteligencia, generando datos que se analizan mediante IA para presentar una imagen global, actualizada en tiempo real. Lógicamente, el resultado proviene de datos no contrastados que aporta personal no entrenado y, que a su vez puede generar información falsa o manipulada. El poder de estas aplicaciones deriva de la cantidad masiva de datos que recopilan, lo que minimiza el impacto de aportaciones individuales falsas.

En el entorno operativo del futuro, se va a incrementar el empleo de aplicaciones que automatizan la localización y monitorización de fuerzas y con ello las capacidades de «targeting colaborativo». En Ucrania se están utilizando PED para detectar y medir la huella sonora del fuego de artillería, que inmediatamente se envían a un sistema que triangula de forma automática su posición (Freese, 2023). Esto se podría combinar con acciones cibernéticas para obtener información de PED de forma involuntaria y así convertir a cualquier persona en el campo de batalla en sensor y dirección de tiro.

Una de las principales amenazas respecto a la PF afecta a la infraestructura vital para la misión, mediante acciones ciberespaciales con repercusión en la dimensión física. La creciente conectividad de esas infraestructuras y la presencia de PED en ellas facilitarán ataques cibernéticos de denegación de acceso, combinados con acciones de *ransomware*[5] o *hacktivismo*[6] por parte de ciberactores no estatales.

4.1.2. Control de drones

Los drones son, por sí mismos, una nueva amenaza en el campo de batalla que excede el alcance de este trabajo. Sin embargo, es necesario recalcar que su empleo se puede dirigir desde dispositivos móviles ya en la actualidad y que esta capacidad va a ampliarse en el futuro: los futuros PED podrán gestionar nubes de drones mediante el empleo de IA.

En el lado opuesto, existen numerosos desarrollos encaminados a proteger a la fuerza de esta amenaza haciendo uso, de nuevo, de las capacidades colaborativas de los PED. Ejemplo de ello es CARPE Dronvm, una aplicación móvil antidron en la que trabaja el Departamento de Defensa estadounidense que permite tomar fotografías de cualquier aeronave y transmitirlas instantáneamente a centros de defensa aérea para su análisis[7].

[5] El *ransomware* es un tipo de *software* malintencionado que impide a los usuarios acceder al sistema y a la información. Exige un rescate para liberar la información.

[6] El *hacktivismo* se trata de la realización de actos maliciosos en internet con fines políticos, religiosos o sociales.

[7] Disponible en: https://www.army.mil/article/268447/usarcent_tests_phone_app_that_detects_unmanned_aerial_systems

4.2. Dimensión virtual

Esta dimensión se asocia a las consecuencias de las actividades relacionadas con los datos digitales, la información, sus procesos y sus sistemas de apoyo. En un mundo digital cada vez más interconectado, protagonizado por el Internet de las Cosas, aumentan las posibilidades de recopilar información y utilizarla contra la fuerza. En el futuro próximo, se dará un paso más hacia el «Internet de todo», en el que infraestructuras, personas, vehículos y objetos estén permanentemente conectados a la red y se enfatizan las comunicaciones máquina-máquina. Cualquier PED comporta riesgos de características únicas para los individuos, las organizaciones y las redes, multiplicando el número de potenciales vectores. Esto se combina con una mayor atomización de sistemas operativos y la presencia en el espacio de las operaciones de PED cada vez más antiguos, no apoyados por el fabricante, pero con capacidades muy significativas.

La mayor sensorización del ser humano implica que el acceso a nuestros PED puede derivar en un conocimiento mucho más profundo de nuestras fuerzas por parte del adversario, que no solo incluirá comportamientos y actividad, sino también sentimientos.

La IA pasará a ser la principal herramienta para automatizar ataques cibernéticos, incluyendo métodos de aprendizaje y programación de *software*. Respecto a la encriptación de datos, se desconoce cuándo va a estar disponible la computación cuántica, pero sí podemos asumir una evolución continua en los sistemas capaces de superar las actuales encriptaciones, por lo que se mantendrá el riesgo asociado al robo de datos. La encriptación no servirá como disuasión, pero sí mitigará su impacto.

4.2.1. Amenazas internas no intencionadas

La amenaza interna no intencionada se considera uno de los peligros de seguridad más graves para empresas privadas, instituciones y organizaciones gubernamentales. Es difícil comprender el alcance y reflejar el peligro que representa esta amenaza, en especial si se combina con acciones de ingeniería social (Greitzer, 2019). En este sentido, la ingeniería social tiene por objetivo obtener información vital para acceder a sistemas informáticos. Esta disciplina se apoya en la psicología humana, particularmente en el aprovechamiento de los sesgos cognitivos, para engañar a la víctima. A diferencia de lo que sucede con otro tipo de amenazas internas, esta actividad se materializa mediante una combinación de acciones secuenciales que van profundizando poco a poco en el conocimiento de la organización y el individuo, tanto mediante interacción personal (que puede ser física o electrónica, haciendo uso de troyanos, *phishing*, etc.) como sin ella (investigación de fuentes abiertas).

4.3. Dimensión cognitiva

La dimensión cognitiva se refiere a las consecuencias en las percepciones, creencias, intereses, decisiones y comportamientos derivados en diferentes audiencias. Toda acción, en cualquiera de los ámbitos de operación, va a tener consecuencias en la dimensión cognitiva. Respecto a los PED, su presencia continua en el campo de batalla va a hacerlos sujetos en la generación de influencia, capaces de crear contenido cada vez más elaborado, y objetos receptores de la influencia externa. Los metaversos, espacios virtuales de interacción, van a suponer una nueva amenaza cognitiva para las fuerzas. Su capacidad inmersiva y la falta de regulación hará a los usuarios susceptibles de acciones de reclutamiento, desinformación y propaganda (Martín, 2023).

4.3.1. Operaciones de influencia ciber-habilitadas

A caballo entre los efectos en la dimensión virtual y la cognitiva, las operaciones de influencia ciberhabilitadas utilizan lo mejor de los más recientes espacios de confrontación en incorporarse al entorno operativo para crear efectos sinérgicos. En la era de la información, estamos permanentemente conectados a redes sociales, agregadores de noticias y buscadores. La principal ventana por la que accedemos a este «infoverso» es nuestro PED.

> En mayo de 2023, un informe sobre el conflicto en Nagorno Karabaj aseveró que se había descubierto spyware en los teléfonos móviles de periodistas y políticos armenios, así como en los de funcionarios de las Naciones Unidas (Krapiva, 2023). Aunque el origen de este ataque no se pudo determinar, su impacto fue doble: por un lado, el acceso a información relevante para el devenir del conflicto; por otro, la desconfianza que generó el empleo de dispositivos electrónicos a toda la comunidad periodística sobre el terreno.

En los últimos años, el tiempo medio diario de acceso a internet se ha estabilizado por encima de las seis horas (tras el máximo histórico que se dio a consecuencia del aislamiento forzado por la epidemia del COVID-19). Las operaciones de influencia ciberhabilitadas aprovechan esta exposición para manipular nuestras percepciones de la realidad y con ello nuestros comportamientos. Del mismo modo que los ciberataques tradicionales preposicionan *malware* en los sistemas objetivo, estas operaciones preposicionan narrativas en la red que empiezan a calar en las audiencias objetivo de forma inadvertida y facilitan la asunción del mensaje manipulado (dirigido por el adversario). A continuación, esta narrativa es amplificada por todo tipo de audiencias que se hacen eco de ella sin comprobar su veracidad, incluso siendo conscientes de su falsedad[8].

[8] Lawson, Anand y Kakkar (2023) afirman que las noticias falsas se expanden por una combinación de presión de grupo y deseo de encajar en grupos sociales, sin importar la ideología de los individuos.

Además de la amenaza que supone esta influencia en las audiencias propias, en el futuro derivará en una era de la posverdad: el esfuerzo necesario para extraer la verdad de un entorno de la información sobresaturado será tan alto, que la verdad dejará de importarle al individuo. Los sistemas de IA de los PED serán los principales gestores de la información que se recibe y presenta, automatizando el filtrado de la información procedente de internet.

4.3.2. Puerta a la desinformación

La manipulación de la información recopilada sobre las fuerzas propias, el empleo de IA para crear contenido falso, la saturación informativa, la desmoralización y la confusión son acciones relacionadas con las operaciones de información que se adaptan muy bien a la interacción a través del ciberespacio que favorecen los PED. El impacto de estas actividades se basa en una continua conexión del individuo a la red. Si bien la interacción humana directa sigue siendo muy válida para objetivos específicos, este modelo de desinformación a través del ciberespacio hace instantáneo el mensaje y globaliza su alcance. Para ello, los PED resultan fundamentales, pues son la puerta de acceso a esta influencia dañina.

Además de un fin en sí misma, la desinformación también se utiliza como medio para generar efectos en otras dimensiones. Mediante las mencionadas acciones de ingeniería social dirigida, un mensaje puede servir de cebo para cometer indiscreciones, violando la OPSEC y poniendo en riesgo a las fuerzas propias.

> En los primeros compases de la invasión de Ucrania, numerosos soldados ucranianos recibieron mensajes de texto que afirmaban que se encontraban rodeados y abandonados. A la vez, mensajes que informaban de la muerte de estos combatientes fueron enviados a sus familias. Estas acciones provocaron una reacción inmediata: tanto los familiares como los propios soldados utilizaron sus PED para tratar de comunicarse con sus seres queridos. Esto supuso un aumento del volumen de comunicaciones en áreas muy determinadas del frente, que fue captado por unidades rusas de guerra electrónica y utilizado para dirigir el fuego de artillería sobre esas posiciones.

5. Gestión del Riesgo

La presencia masiva de PED en el campo de batalla del futuro se convierte en una amenaza continua y evolutiva para la Fuerza. La gestión del riesgo debe adaptarse a la amenaza y mitigar su impacto hasta permitir el cumplimiento de la misión. La PF entiende que siempre existe un riesgo mínimo;

sin embargo, de no mitigar sus efectos, los PED pueden tornar ese riesgo base en inasumible para la Fuerza. Dada la capacidad multidominio de los PED, los factores que se mencionan a continuación son, en muchos casos, transversales y afectan a diversas áreas de capacidad de la Fuerza.

Las soluciones materiales para adaptarnos a esta nueva situación no pueden ser disruptivas. Como afirma Villanueva (2023) respecto a la revolución militar de la información, «en todo lo relativo a escenarios futuros, entornos operativos y planeamiento de las adquisiciones, el proceso de cambio acelerado [...] dificultará sobremanera hacer las elecciones correctas». El éxito debe provenir del equilibrio entre tecnologías presentes y futuras, combinando lo mejor de los nuevos desarrollos con la fiabilidad y resiliencia del material probado.

Una medida pasiva para denegar al oponente información vital es incorporar una gestión efectiva de la huella visual, electromagnética y digital que generan nuestras fuerzas. Esto puede incluir implementar medidas de OPSEC, disciplina en las comunicaciones o camuflaje. Nada de esto es nuevo, pero sí puede serlo la forma de plasmarlo, aplicando las ventajas que ofrecen las nuevas tecnologías: normalización de VPN en las redes públicas del personal desplegado, camuflaje electromagnético, análisis de sentimiento de redes sociales alrededor de nuestras fuerzas, integración de capas de seguridad corporativa en los sistemas privados, implantación de un ecosistema de aplicaciones para la comunicación interna en el frente o nubes privadas encriptadas para el uso de PED integrados en la nube de combate son solo algunos de los ejemplos que podemos esperar ver en los próximos años.

Dentro de la infraestructura vital para la misión, deberá tenerse en cuenta a los sistemas satelitales, sean civiles o militares, no solo desde el punto de vista de la seguridad física, sino desde la seguridad de acceso a todas las capacidades que ofrecen. Esto contribuiría a asegurar redes de comunicaciones resilientes e independientes, vitales en el futuro espacio de las operaciones.

La Fuerza también debe contar con los mecanismos necesarios para dotarse ágilmente de aplicaciones móviles que respondan a las necesidades del frente, adoptando los conceptos de combate colaborativo y descentralizado en beneficio propio.

Aunque pueda resultar una obviedad, una de las principales medidas para mitigar la amenaza derivada del uso de PED es conocerlos. Esta simple afirmación conlleva una enorme complejidad en su ejecución: en el entorno operativo futuro van a coexistir una miríada de aparatos diferentes: PED modulares adaptados a los requerimientos del usuario, sistemas operativos de código abierto no actualizados, *software* específico desarrollado por IA,

convivencia de equipos obsoletos con otros de última generación... La prioridad debe enfocarse a conocerlos como entes conectados: los PED serán entes físicos, pero su valor proviene de su interacción en y a través del ciberespacio. En el ciberespacio, la mitigación de riesgos debe alcanzarse mediante tres líneas de acción: proteger la seguridad del PED, proteger los datos y proteger la privacidad del usuario.

La protección de los PED, en particular la de los dispositivos privados, va a necesitar la participación y la mentalización de sus usuarios, unida a programas de revisión continua por parte de la organización. Idealmente, todo PED en la fuerza propia debería estar identificado y su seguridad actualizada para evitar ataques de denegación de servicio, filtración de tráfico o que comprometan a otros equipos en la red.

La protección de los datos implica mantener la confidencialidad, integridad y disponibilidad de los datos que se almacenan o pasan por el PED, lo que también supone aumentar la resiliencia de la infraestructura de comunicaciones de las FAS. El diseño de las redes y el material que soporten los sistemas de información y comunicaciones debe alcanzar un adecuado equilibrio entre agilidad en el acceso y seguridad de la información.

La protección de la privacidad se complementa con las anteriores y trata de evitar vulnerabilidades que afectan al individuo y, en general, tienen un impacto cognitivo mayor. De nuevo, será necesaria la colaboración de los usuarios a la hora de limitar el empleo malintencionado de los sensores activos de sus PED y, con ello, la recopilación automática de información.

La nueva generación de PED está cambiando las amenazas a las que se enfrenta la fuerza en el ciberespacio, por lo que la PF debe entender las vulnerabilidades que van a existir en un entorno móvil en constante crecimiento. Para garantizar un entorno seguro para los PED, es necesario tener en cuenta la movilidad de estos dispositivos, la seguridad en los correos electrónicos, la protección frente a amenazas originadas en sistemas remotos, redes privadas virtuales y las nubes de datos. En el entorno de las FAS, esto supone dotar a los PED privados de capas de seguridad *ad hoc*, o bien limitar su uso. Incluso con aparatos corporativos existen riesgos, asociados a su empleo en el ámbito particular, por lo que la formación y la mentalización van a seguir teniendo un papel primordial.

Esta amenaza no va a remitir en el futuro, al contrario. La presencia de PED, cada vez más potente en y alrededor de la organización, se va a utilizar para monitorizar y elegir a la víctima más propicia y acceder de forma remota a redes de baja encriptación. Frente a ello, los sistemas de ciberseguridad deben garantizar la compartimentación de información en función del usuario, para limitar el impacto de estas acciones y evitar que una falla afecte

a toda la organización. Además, la cultura de ciberseguridad debería presentar un enfoque claro hacia el factor humano, que contribuya a detectar estas posibles amenazas, tanto de entes maliciosos como de entes ininten-cionales. Asimismo, el refuerzo de las capacidades de contrainteligencia en el ciberespacio en apoyo a la PF permitiría mejorar los tiempos de reacción y contribuiría a la identificación temprana de amenazas potenciales en sus fases de preparación, antes de que se materialicen. El conocimiento de la situación, mediante herramientas de análisis y valoración del entorno de la información, contribuiría a reducir riesgos en los ámbitos ciberespacial y cognitivo.

La lucha contra la desinformación en el seno de nuestras tropas no se puede contemplar como una actividad de PF aislada. Es necesario mejorar la coordinación que existe con el resto de instrumentos de poder del Estado, en especial los relacionados con la información, e implicar al sector privado y a la sociedad civil para incrementar la resiliencia cognitiva de la Fuerza, minimizando así el impacto de estas campañas.

En el futuro, se requerirá una mayor transparencia de la actuación propia en las operaciones (frente al exceso de clasificación de información que, en cualquier caso, podría terminar en los medios), así como desarrollar y potenciar capacidades relacionadas con las operaciones de información. La presencia permanente de dispositivos que grabarán toda acción supone que la actuación propia deberá ser impecable en lo general y en lo particular. Para transmitir esa realidad, se deben reforzar los equipos de operaciones de información propios, con perfiles de apoyo como los cámaras tácticos o los productores de contenido multimedia, que sepan captar y presentar la acción propia y contrarrestar acciones maliciosas que vayan contra la seguridad de la organización.

Al contrario de lo que pudiera parecer, una de las recomendaciones para mitigar el impacto de la desinformación y sus consecuencias en el seno de la Fuerza Conjunta es minimizar las prohibiciones de uso de teléfonos móviles y las restricciones de acceso a redes sociales (Cohen, 2021: 88). Las prohibiciones contribuyen a reducir algunos riesgos, pero pueden conllevar consecuencias indeseadas: afectar al componente moral de la fuerza de combate, favorecer la presencia de PED no regulados en el seno de la Fuerza o provocar una reducción en la confianza institucional.

Frente a esta opción, medidas relacionadas con la formación y la mentalización parecen funcionar mejor. La alfabetización mediática e informacional, los estudios de caso y el adiestramiento en simuladores enfocados al ámbito cognitivo contribuyen a reforzar las capacidades de juicio crítico individual y colectivo. Estas medidas se pueden complementar mediante actividades de formación contra la desinformación para las familias.

Otra herramienta muy útil para verificar la información multimedia y limitar el impacto de los *deep fakes*, una vez se generalice la generación de contenido falso mediante IA, será el uso de «marcas de agua digitales» que certifiquen la procedencia y veracidad de estos materiales. Además, las FAS deben entender y adaptarse a la presencia de los últimos PED de mercado y valorar su impacto cognitivo, especialmente una vez se normalicen los dispositivos que potencian la inmersión sensorial, como los aparatos de realidad virtual, realidad aumentada y los interfaces hombre-máquina.

6. Consideraciones finales

Los dispositivos móviles personales no van a separarse del ser humano. De la misma manera que nuestros sentidos nos sirven para percibir el entorno físico, los PED nos ayudan a percibir el entorno digital, actuando de nexo entre la realidad física y las realidades virtual y cognitiva. Dada su cercanía al individuo, son el primer recurso con el que se accede a la identidad ciberespacial y el primero con el que se captura y digitaliza el mundo que nos rodea.

La PF frente a estos dispositivos debe plantearse desde una perspectiva integradora, no confrontacional, que aproveche las ventajas que ofrecen y minimicen los riesgos derivados de su uso. Debe asumir la presencia continua de PED en y alrededor de la Fuerza y servirse de sus capacidades, que serán cada vez más potentes, para contribuir a las operaciones. La revolución en el modelo de soldado de los próximos años no se derivará de sus capacidades físicas, sino que provendrá de su sensorización y conectividad. Dispondrá de PED que mirarán hacia sí mismo (monitores de actividad, sensores biométricos, interfaces) y hacia el exterior (dispositivos de realidad aumentada, sistemas de comunicación, aparatos de grabación multimedia), con una gestión de la información automatizada mediante IA que los hará parte de la nube de combate, convirtiéndolos en sensor y en arma.

La PF debe adaptarse a esta realidad, en la que todo individuo puede portar diversas células de sistemas distribuidos altamente sofisticados. En el entorno operativo futuro, la difícil distinción entre civil o militar deberá sortearse mediante sistemas no letales y medidas pasivas avanzadas que mejoren la resiliencia propia, en especial en lo que respecta a la protección de la información. Las medidas más extremas de limitación a la conectividad personal (bien sea mediante acciones de guerra electrónica, prohibición de PED o destrucción física) serán cada vez menos eficaces por la capacidad de adaptación que van a alcanzar, su miniaturización y el alto número de dispositivos disponibles.

El factor humano seguirá desempeñando un papel clave: la mentalización, la disciplina de empleo y la capacidad de juicio crítico serán las bases sobre las que construir redes resilientes, sistemas inteligentes para la

identificación de dispositivos, acceso a la información basado en necesidad de uso, mínima clasificación, modelos ágiles de obtención de hardware y *software*, capacidades de información preparadas para las operaciones en el ciberespacio y el ámbito cognitivo, así como modelos de mando y control adaptados a la nueva forma de abordar las operaciones, distribuida y colaborativa.

No olvidemos la lección que nos deja el caballo de Troya: los PED son una puerta abierta a riesgos multidominio. La llave para asegurar la PF esta en nuestras manos.

7. Bibliografía

Colom-Piella, G. (2023). The Bear in the Labyrinth. *RUSI Journal*. Vol. 167, 6/7. Londres, Royal United Services Institute.

Cohen, R. *et al.* (2021). *Combating Foreign Disinformation on Social Media: Study Overview and Conclusions.* Santa Mónica, RAND Corporation.

Estado Mayor de la Defensa. (2019). *Protección de la Fuerza. PDC-3.14.* Madrid, Ministerio de Defensa. Disponible en: https://emad.defensa.gob.es/Galerias/CCDC/files/PDC-314_PROTECCION_DE_LA_FUERZA_para-web_09003a9980b53cd7.pdf

Freese, K. (2023). TRADOC: Smart Phones Playing Prominent Role in Russia-Ukraine War. *Red Diamond. TRADOC G-2 Newsletter.* Vol. 14, 2. Virginia, U.S. Army Training and Doctrine Command.

García, F. *et al.* (2011). Señas de identidad del 'nativo digital'. Una aproximación teórica para conocer las claves de su unicidad. *Cuadernos de documentación multimedia.* Madrid, Universidad Complutense de Madrid.

Greitzer, F. (2019). Insider Threats: It's the HUMAN, Stupid!. *NCS '19: Proceedings of the Northwest Cybersecurity Symposium,* pp. 8-10. New York, Association for Computing Machinery. DOI: 10.1145/3332448.3332458

Horbyk, R. (2022). 'The war phone'. Mobile communication on the frontline in Eastern Ukraine. *Digital War*. DOI: 10.1057/s42984-022-00049-2

Jensen, B. y Paschkewitz, J. (2019). Mosaic Warfare: Small and Scalable are beautiful. *Special Series–Next War*. *War on the Rocks.* Washington, War on the Rocks Media, LLC.

Kaprina, N. (2023). *Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict*. Access Now.

Kemp, S. (2023). Digital 2023: Global Overview Report. *DataReportal*. Disponible en: https://datareportal.com/reports/digital-2023-global-overview-report

Klim, V. (2023). Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack. *The New York Times*. Disponible en: *https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html*

Lawson, M. *et al.* (2023). Tribalism and Tribulations: The Social Costs of Not Sharing Fake News. *Journal of Experimental Psychology: General*. 152, pp. 611–631. DOI: 10.1037/xge0001374

Martín, A. (2023). *El metaverso: potenciales riesgos y amenazas para la paz y la seguridad, y su contagio en el mundo re<<<<<<<<<al*. Documento de opinión 40/2023. Madrid, Instituto Español de Estudios Estratégicos.

Ministerio de Defensa. (2021). *Panorama de tendencias geopolíticas. Horizonte 2040*. 2.ª ed. Madrid, Ministerio de Defensa.

National Intelligence Council. (2021). *Global Trends 2040. A more contested world.* Cosimo Reports. ISBN 978-1-929667-33-8.

Olejnik, L. (2022). Smartphones Blur the Line Between Civilian and Combatant. *Wired*. Disponible en: https://www.wired.com/story/smartphones-ukraine-civilian-combatant/

OTAN. (2022). *AJP-01 Edition F Version 1. Allied Joint Doctrine*. Bruselas, NATO Standardization Office.

Prensky, M. (2001). Digital Natives, Digital immigrants Part 1. *On The Horizon*. Vol. 9, 5, pp. 1-6. DOI: 10.1108/10748120110424816

Reding, D. *et al.* (2023). Science & Technology Trends 2023-2043. Vol. 1. Bruselas, NATO Science & Technology Organization.

Villanueva, C. (2023). La Tercera Revolución Militar: la Revolución Militar de la Información. *Revista Ejércitos.* 52. Guipúzcoa.

Virgilio (s. f.). *La Eneida.* De Ochoa, E. (trad.). Ediciones elaleph.com.

Capítulo 5

Dirección y gestión de seguridad frente a nuevas amenazas tecnológicas

José Luis Bolaños Ventosa

Resumen

La digitalización de nuestra sociedad y el desarrollo tecnológico que le acompaña ha supuesto una revolución en la historia de la humanidad. El hombre ha creado una nueva dimensión, la digital, que no tiene fronteras y donde las leyes tienen una difícil aplicación. Este escenario, que ha supuesto una aportación de mejoras en todos los ámbitos, también ha venido acompañado de un nuevo entorno de riesgos digitales, que suponen una amenaza sin precedentes para nuestra sociedad por su frecuencia, impacto y graves consecuencias.

El mundo de la empresa, por su agilidad, dinamismo y eficiencia, ha desarrollado modelos de gestión del riesgo colaborativos, para garantizar el desarrollo de sus negocios.

Vamos a compartir, a continuación, algunos ejemplos de modelos de seguridad y un caso práctico de su implantación en una empresa de infraestructuras críticas del sector de la energía, de forma que puedan servir de referencia al ámbito de la Defensa.

Palabras clave

Servicios Esenciales, Protección de Infraestructuras Críticas, Ciberseguridad, Resiliencia, Seguridad Global.

Address and manage security in the face of emerging technology threats

Abstract

The digitalization of our society and the technological development that accompanies it, has brought about a revolution in the history of mankind. Man has created a new dimension, the digital one, which has no borders and where laws are difficult to apply. This scenario, which has brought improvements in all areas, has also been accompanied by a new environment of digital risks, which pose an unprecedented threat to our society due to their frequency, impact, and serious consequences.

The business world, due to its agility, dynamism, and efficiency, has developed collaborative risk management models to guarantee the development of its businesses.

We will now share some examples of security models and a practical case of their implementation in a critical infrastructure company in the energy sector, so that they can serve as a reference for the defense sector.

Keywords

Essential Services, Critical Infrastructure Protection, Cybersecurity, Resilience, Global Security.

1. Introducción

El sector de la energía eléctrica no es solamente importante por el impacto de su actividad en la economía, sino porque proporciona servicios esenciales, de forma continua, al conjunto de la sociedad. En un mundo tan tecnificado, la dependencia de la energía eléctrica es cada vez mayor y, por tanto, su falta es cada vez más crítica.

Los sistemas eléctricos han sido diseñados, desde su origen, para la interconexión con otras redes nacionales y de otros países, disponen de infraestructuras redundantes que deben cubrir en tiempo real toda la demanda de energía del mercado eléctrico y, en particular, la que necesitan otros servicios esenciales, como son las redes de comunicación, los sistemas de información, la sanidad, la banca o las Administraciones Públicas.

Este complejo sistema eléctrico incluye el proceso de generación de electricidad (desde diferentes fuentes como son hidráulica, nuclear, térmica convencional, eólica o solar), el transporte de electricidad, a través de las redes de alta tensión y la distribución mediante una red muy capilarizada y redundante que lleva la energía hasta los consumidores finales. Todo ello esta soportado por un complejo conjunto de infraestructuras físicas y digitales que son gestionadas a través de los llamados centros de gestión de la red eléctrica que operan, de forma permanente, la demanda de energía del mercado.

Esta larga y compleja cadena de suministro, que incluye instalaciones muy sensibles, forma parte de un ecosistema en donde todas las empresas eléctricas interactúan y donde existe también una amplia dependencia de otros servicios esenciales, entre los que se destacan las redes de comunicaciones y los sistemas de información.

Podemos decir que el conjunto del sistema eléctrico nacional, que esta a su vez interconectado con el resto de Europa y Marruecos, conforma una red de empresas, mayoritariamente privadas, que tienen que funcionar de forma sincronizada, en una relación de dependencia con multitud de empresas de servicios.

Para que el conjunto del sistema eléctrico sea seguro y resiliente hace falta que toda la red tenga unos niveles homogéneos y equivalentes de seguridad, con los que se pueda garantizar la integridad y protección del mismo.

En los últimos veinte años se ha producido un proceso de mejora y optimización de la seguridad de nuestras infraestructuras críticas, que ha sido el resultado del desarrollo e implantación de diferentes directivas europeas en el ámbito de la seguridad física, la ciberseguridad y la resiliencia, que se han desplegado en los diferentes Estados miembro de la Unión Europea,

mediante la correspondiente trasposición de las mismas y el desarrollo de las Estrategias Nacionales de Seguridad y Ciberseguridad.

El resultado de este trabajo colaborativo entre las Administraciones públicas y las empresas, promovido por la Comisión Europea y liderado en nuestro país por el Centro Nacional de Protección de Infraestructuras Críticas, ha contribuido, de forma decisiva, a que España haya aumentado significativamente el nivel de madurez en seguridad de nuestras infraestructuras críticas.

2. Modelo de Protección de Infraestructuras Críticas (PIC)

2.1. Contexto

Los graves atentados terroristas de Nueva York en 2001 y posteriormente los atentados de Madrid en 2004 y Londres en 2005 pusieron de manifiesto la gran vulnerabilidad de nuestra sociedad para hacer frente a ataques suicidas que buscan causar el mayor daño posible y supuso un punto de inflexión en la forma de entender la seguridad.

Si bien en el ámbito de la Unión Europea las competencias de seguridad y defensa son exclusivas de los Estados miembros, la globalidad de la amenaza terrorista y la necesidad de una respuesta conjunta, motivaron que se lanzara por la Comisión Europea un proyecto para definir, desarrollar e implantar un Modelo común de Protección de Infraestructuras Críticas (en adelante, Modelo PIC).

Entre las infraestructuras críticas (en adelante IC), destacan las energéticas, los transportes, las comunicaciones, las redes y sistemas de información, la banca o el sector agua, entre otras.

Las IC están interconectadas entre sí y a su vez entre los diferentes países de la Unión Europea, así como con otros países limítrofes. El daño severo o destrucción de alguna de estas IC puede provocar un efecto cascada en el resto de países.

La interdependencia entre las mismas y la transversalidad entre los diferentes países de la Unión Europea y limítrofes, hacen que la tarea de proteger las IC, sea especialmente compleja y que no se pueda entender la misma sin una firme colaboración entre los distintos países de la Unión y entre las Administraciones públicas y las empresas en cada uno de los Estados miembros.

La Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, define y desarrolla un

modelo de seguridad, colaborativo e integrado, que sirva de referencia a los Estados miembros y a las empresas operadoras para garantizar la prestación de los servicios esenciales en Europa.

La trasposición de esta Directiva europea en España se concreta con la promulgación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Esta ley supone un avance fundamental, al profundizar y concretar el enfoque y metodologías necesarias para desarrollar un Modelo PIC con un alto nivel de madurez. Hecho diferencial de esta norma es que habla por vez primera de integrar la gestión de los riesgos de seguridad física y los cibernéticos, de forma que se pueda tener una visión global de los mismos.

2.2. Componentes del Modelo PIC

La ley PIC establece la estrategia y estructuras adecuadas, que permitan dirigir y coordinar a los diferentes organismos de la Administración Pública en el ámbito de la protección de las IC, con el fin de mejorar las capacidades de prevención, protección y respuesta frente a atentados terroristas u otras amenazas deliberadas que puedan afectar a las IC. Fomenta la participación e implicación de las empresas propietarias u operadoras de IC, todo ello con el objetivo de mejorar la protección de la población a través de la prestación de los servicios esenciales. Esta ley no tiene régimen sancionador, pues se construye sobre el «principio de confianza» entre la Administración competente y las empresas operadoras de servicios esenciales.

2.2.1. Catálogo nacional de infraestructuras críticas

La Secretaría de Estado de Seguridad es la responsable de la elaboración y mantenimiento del catálogo nacional de infraestructuras estratégicas, donde se incluye toda la información y valoración correspondiente a las IC en nuestro país. En la identificación del catálogo intervienen las diferentes Administraciones públicas, así como las empresas operadoras o propietarias de IC. La Secretaría de Estado realiza la designación de la empresa como operador crítico.

2.2.2. Análisis de riesgos

Tanto la Administración competente, en el nivel estratégico sectorial, como los operadores de empresas de IC deben realizar, de forma periódica, el análisis que permita la identificación y clasificación de amenazas, riesgos y vulnerabilidades, que puedan afectar a los activos críticos.

2.2.3. Gobernanza y organización

Se establecen los siguientes organismos para garantizar una adecuada gestión del modelo PIC:

- Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)
  Integrado dentro de la Secretaría de Estado de Seguridad (SES) del Ministerio del Interior, funciona como organismo técnico especializado para la coordinación y gestión del modelo en España, entre las Administraciones implicadas y empresas operadoras, así como la colaboración con otros Estados miembros.
- Comisión Nacional para la Protección de Infraestructuras Críticas
  Órgano colegiado adscrito a la SES, tiene como responsabilidades principales designar los operadores críticos que se propongan y aprobar los diferentes Planes Estratégicos Sectoriales.
- Grupo Interdepartamental para la Protección de Infraestructuras Críticas
  Elabora los diferentes Planes Estratégicos Sectoriales y propone a la Comisión la designación de operadores críticos por cada uno de los sectores estratégicos definidos.
- Empresas Operadoras de Infraestructuras Críticas
  Implantan los medios y recursos necesarios para proteger las IC que gestionan. Participan con el Grupo Interdepartamental PIC en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgo sectoriales de su ámbito de competencia. Elaboran el Plan de Seguridad del Operador e implementan y mantienen los Planes de Protección Específicos, por cada una de las infraestructuras consideradas como críticas dentro del catálogo. Designan un responsable de Seguridad y Enlace, como punto de contacto entre el CNPIC y las Fuerzas y Cuerpos de Seguridad. Igualmente, designan un delegado de Seguridad por cada una de las IC, que es responsable de la seguridad de la misma.

2.2.4. Planificación de seguridad

Con objeto de establecer un tratamiento homogéneo, sostenible y auditable a todas las IC, se establece una planificación en diferentes niveles, que implica y compromete tanto a las Administraciones públicas como a los operadores de las IC. Tiene tres niveles:

- Nivel estratégico
  Lo componen el Plan Nacional de Protección de Infraestructuras Críticas (PNPIC) y los Planes Estratégicos Sectoriales (PES) (vinculados a cada uno de los sectores estratégicos definidos en el PNPIC). Estos Planes son competencia exclusiva de la SES y el CNPIC, pero para su elaboración se

apoyan en el resto de Administraciones públicas implicadas y las propias empresas operadores críticos.

- Nivel táctico
  El Plan de Seguridad del Operador (PSO) es elaborado por el operador crítico y aprobado por el CNPIC. Recoge todas las IC del operador, los riesgos generales de seguridad identificados (físicos y digitales), así como las medidas de gobierno, organizativas, humanas y técnicas, aplicables a la empresa para gestionar sus riesgos de seguridad.
- Nivel operativo
  Los Planes de Protección Específicos (PPE) son competencia del operador y se aprueban por el CNPIC. Hay un PPE por cada una de las IC. En el mismo se describen los activos a proteger (características, entorno), efectos que puede producir su daño e interdependencias con otras IC. Dispone de un análisis de riesgos (físicos y cibernéticos) y establece las medidas de seguridad específicas, como son la organización de la seguridad, con funciones y responsabilidades, los procedimientos y protocolos de actuación para la prevención, protección y respuesta ante incidentes de seguridad e incluye las medidas de protección física y cibernética, tanto las que tienen carácter permanente como las de carácter temporal.
  El Plan de Apoyo Operativo (PAO) es responsabilidad de las Fuerzas y Cuerpos de Seguridad. En él se detallan las medidas de aplicación específicas por las Fuerzas y Cuerpos de Seguridad, para cada una de las IC en su ámbito de competencias.

2.3. Enfoque de la ciberseguridad en el Modelo PIC

El despliegue de la digitalización de nuestra sociedad y el incremento exponencial de los riesgos cibernéticos y sus consecuencias han hecho necesario poner el foco en la protección de las redes y sistemas de información con especial énfasis en aquellas que afectan a la prestación de servicios esenciales. La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, establece medidas concretas para incrementar el nivel común de seguridad en las redes y sistemas de información dentro de la Unión, a fin de mejorar el funcionamiento, competitividad y sostenibilidad del mercado interior.

Incorpora las condiciones básicas comunes para el desarrollo de capacidades, planificación, intercambio de información, cooperación y requerimientos de seguridad, tanto para los operadores de servicios esenciales como para los proveedores de servicios digitales.

La trasposición de la Directiva NIS a nuestro país se recoge en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y

sistemas de información, en el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Con esta normativa se establecen y regulan la seguridad de las redes y sistemas de información, la comunicación de incidentes de seguridad, la gestión de los mismos y la supervisión del cumplimiento de las obligaciones por parte de los operadores de servicios esenciales, así como de los proveedores de servicios digitales en nuestro país.

Los nuevos requerimientos de ciberseguridad, para las empresas operadoras de servicios esenciales, son los siguientes:

2.3.1. Identificación de servicios y operadores de servicios esenciales

Incluye aquellas empresas públicas o privadas que prestan servicios esenciales para el mantenimiento de actividades sociales o económicas críticas y que dependen de las redes y sistemas de información para prestar sus servicios.

Tienen una especial consideración en la Defensa Nacional aquellos proveedores de servicios esenciales básicos para el funcionamiento de Ministerio de Defensa o para la operatividad de las Fuerzas Armadas que puedan tener incidencia en la Defensa Nacional. Estos son identificados por el Ministerio de Defensa, que se encarga de su comunicación, a efectos de su designación a la Comisión Nacional para la Protección de Infraestructuras Críticas.

2.3.2. Gobernanza y organización

La Estrategia de Ciberseguridad Nacional, complementaria y alineada con la Estrategia de Seguridad Nacional, establece, a alto nivel, los objetivos y prioridades, un marco de gobierno y las capacidades para la preparación, respuesta y recuperación ante incidentes graves de ciberseguridad.

- Autoridad Competente
  El Ministerio del Interior, a través de la SES, para todos los operadores de servicios esenciales incluidos dentro de la Ley PIC, es el responsable de establecer las medidas y obligaciones específicas para garantizar la seguridad de las redes y sistemas de información, facilitar instrucciones técnicas y guías específicas sobre el contenido de las obligaciones establecidas y supervisar el cumplimiento de las mismas, ejerciendo la potestad sancionadora en caso de incumplimiento. Se designa como Punto de Contacto Único al Departamento de Seguridad Nacional, del Consejo de Seguridad Nacional, para la coordinación en ciberseguridad con otros Estados miembro.

- Equipos de respuesta a incidentes de seguridad informática: CSIRT (Computer Security Incident Response Team)
  Sus funciones principales son, la supervisión de los incidentes cibernéticos a nivel nacional, la difusión de alertas tempranas, el aviso e información sobre riesgos e incidentes a las partes interesadas, la respuesta ante incidentes y el análisis de riesgos e incidentes. Participan en la red CSIRT nacional e internacional y colaboran con el sector privado para la adopción y utilización de buenas prácticas.
  Para la gestión de todos los incidentes que afecten a los operadores críticos se designa al INCIBE-CERT operado conjuntamente por el INCIBE y el CNPIC. El ESPDEF-CERT del Ministerio de Defensa colaborará con los anteriores en situaciones en las que se requiera su apoyo para la gestión de incidentes que afecten a la Defensa Nacional.

2.3.3. Medidas de ciberseguridad para los operadores esenciales

Las empresas de servicios esenciales y los proveedores de servicios digitales adoptan medidas técnicas y organizativas adecuadas y proporcionadas para hacer una gestión óptima de los riesgos de seguridad que puedan afectar a las redes y sistemas de información. Deben tener aprobada una Política de Ciberseguridad, en la que se contemple la seguridad de forma integral (física y cibernética), el proceso completo de gestión de riesgos (la prevención, respuesta y recuperación), las líneas de defensa, la revisión del modelo de ciberseguridad y la segregación de tareas. Es fundamental considerar la dependencia e interdependencias, así como la prestación de servicios y suministros contratados por el operador con terceros.

- Responsable de Seguridad de la Información (RSI)
  Los operadores designan una persona como punto de contacto con la Autoridad competente y con los CSIRT de referencia. En el ámbito de su empresa es responsable de desarrollar y proponer las políticas de seguridad, las medidas organizativas, técnicas y humanas y supervisa su implantación.

- Notificación de incidentes
  Aquellos que puedan tener efectos perturbadores significativos en los servicios esenciales, cuyo impacto sea crítico, muy alto o alto, deberán ser comunicados por el RSI al CSIRT de forma inmediata.
  Cuando un operador tenga una incidencia que pueda afectar a la Defensa Nacional, pondrá en conocimiento del hecho de forma inmediata al CSIRT de referencia, quien dará traslado al ESPDEF-CERT del Mando Conjunto del Ciberespacio.

- Gestión de incidentes de seguridad
  Los operadores de servicios esenciales y los proveedores de servicios digitales deben gestionar y resolver los incidentes que afecten a las redes

y servicios de información. A su finalización deben elaborar un informe de detalle con la evolución de los hechos, la valoración de probabilidad de su repetición y las medidas correctoras aplicadas.

- Supervisión de los operadores de servicios esenciales
  Las autoridades competentes supervisan el cumplimiento de las obligaciones aplicables a operadores de servicios esenciales y proveedores de servicios digitales. Tienen la potestad de sancionar los incumplimientos que se puedan producir en la aplicación de la normativa.

3. El modelo de gestión de riesgos Enterprise Security Risk Management (ESRM)

3.1. Introducción

ASIS International es la organización de profesionales de seguridad más importante e influyente en el ámbito internacional. Sensible a los importantísimos cambios que se han producido durante las dos últimas décadas, con el incremento en la frecuencia y gravedad de los riesgos digitales, de las crisis geopolíticas y las catástrofes naturales, ha desarrollado un modelo de seguridad de referencia, para que las organizaciones públicas y privadas puedan implantarlo, independiente de su tamaño, con el objeto de alcanzar un alto nivel de madurez en seguridad global.

ESRM contempla una nueva filosofía y metodología para la gestión de los programas de seguridad global en la empresa, mediante el uso de principios de la gestión de riesgos. Pone el foco en la creación de una relación sólida entre los responsables de seguridad y los directivos responsables de los activos de la empresa, con el objeto de implicar y responsabilizar a estos últimos en la gestión de los riesgos de seguridad que afectan a su negocio. Esta metodología esta contrastada en la práctica de empresas de referencia en todos los sectores y geografías.

Busca que la estrategia de la seguridad esté alineada con la estrategia general de la empresa, su misión, visión, valores y objetivos. Tiene un enfoque basado en el riesgo, aplicable a todos los ámbitos de la seguridad, física, cibernética, fraude, crisis y continuidad de negocio. Define como debe ser un programa progresivo y escalable de seguridad, planifica la seguridad a través de iniciativas concretas, traslada el conocimiento del rol de la seguridad a las áreas de negocio y consolida los mecanismos de reporte e información sistemáticos sobre riesgos de seguridad a los órganos de dirección y gobierno de la empresa.

3.2. Principios del ESRM

Con una visión estratégica y no táctica, se fundamenta en crear vínculos firmes entre los objetivos empresariales y la gestión de riesgos de seguridad. Se basa en el principio de responsabilidad compartida, entre el área de seguridad y los directivos responsables de los activos, siendo estos últimos los responsables de la decisión final.

Permite obtener un conocimiento profundo de la organización, de sus diferentes grupos de interés (*stakeholders*) y entender qué es lo que consideran importante sobre los activos, estrategias y objetivos. De igual forma, proporciona una visión de alto nivel basada en la gestión de riesgos globales de seguridad, a través del conocimiento de estos. Proporciona estructuras de seguridad que están basadas en las mejores prácticas para la protección de los activos en todos los ámbitos.

3.3. Ciclo de vida del ESRM

El modelo se articula sobre la base de cuatro procesos básicos:

3.3.1. Identificación y priorización de activos

Se define un activo como cualquier elemento que aporte valor a la organización. Los activos tienen propietarios dentro de la organización, que son los responsables de mitigar los riesgos que les puedan afectar hasta un nivel aceptable para la empresa. Los activos deben valorarse, catalogarse y priorizarse, basándose en las metas y objetivos de la organización. El valor del activo puede medirse por el coste de reposición del mismo o por el impacto operacional o reputacional de su indisponibilidad.

3.3.2. Identificación y priorización de riesgos

Este proceso implica la realización de análisis de riesgos de seguridad para los activos. Este análisis incluye las amenazas, vulnerabilidades, impacto, probabilidades y valor de los activos. El nivel de riesgo es establecido mediante la vinculación del riesgo identificado con el valor del riesgo aceptable. Las áreas que superan este valor son calificadas como de alto riesgo. El proceso de identificación y clasificación de los riesgos altos, se conoce como priorización de riesgos.

3.3.3. Mitigación de los riesgos priorizados

Incluye los controles que son necesarios adoptar para reducir un riesgo de nivel alto a un riesgo de nivel aceptable. La mitigación es una de las

categorías de tratamiento del riesgo. Las otras son la aceptación, la evitación o la transferencia del riesgo.

En el caso de la aceptación del riesgo, se admiten los escenarios de riesgo basándose en el nivel de tolerancia de la empresa. El riesgo se puede transferir a través de contratos de aseguramiento o por la externalización de actividades a terceros. En cuanto a la evitación, se consigue mediante el cambio, modificación o cierre de diferentes procesos o áreas de negocio.

En la mitigación del riesgo se pone el foco en la reducción de la probabilidad o impacto del riesgo mediante controles adicionales y medidas que consiguen reducir el nivel de riesgo a unos términos aceptables. Ejemplos de medidas de mitigación son los controles de acceso, sistemas de videovigilancia, formación y entrenamiento en prevención de pérdidas, entre otros.

3.3.4. Mejora continua del programa de seguridad

El ciclo de vida ESRM está fundamentado en un enfoque reiterado de evaluación, mitigación y mejora continua del proceso de gestión de riesgos. El intercambio de información de seguridad entre los responsables de los activos, *stakeholders* y el director de seguridad, la capacidad de gestión de incidentes, así como su investigación y análisis, son elementos fundamentales de este proceso.

La gestión de incidentes incluye la respuesta y el seguimiento hasta su resolución. En el análisis y la valoración posterior se identifica la causa raíz, se establecen y priorizan los controles de mitigación y se miden los tiempos de respuesta. Esto permite detectar riesgos emergentes, identificar puntos de mejora y compartir las lecciones aprendidas con el resto de la organización.

3.4. Proceso de implantación ESRM

El primer paso es realizar una evaluación completa de la seguridad global de la empresa, mediante la utilización de la herramienta de Evaluación de nivel de madurez en ESRM, desarrollada por ASIS International.

El modelo establece seis categorías evaluables que tienen establecidos diferentes controles. En cada control se establece una puntuación en función de las evidencias que se puedan documentar. El resultado de la valoración permite establecer un *rating* en uno de los siguientes niveles: Inicial, Repetible, Definido, Gestionado y Optimizado. Las categorías sobre las que se miden los controles para evidenciar el nivel de madurez son las siguientes:

3.4.1. Estrategia de seguridad global

Analiza la misión, objetivos y el compromiso de aplicación del ESRM por parte de la empresa. La Estrategia de Seguridad Global debe incluir, entre otros, la adopción de un modelo de riesgo, la asignación de recursos y el desarrollo de las capacidades necesarias para su implantación.

3.4.2. Gobernanza del programa

Valora la constitución de un Comité de Seguridad Global Corporativo, como máximo órgano de gobierno y toma de decisiones a nivel estratégico. Formado por los directivos responsables de los activos y dirección de seguridad, establece el nivel de riesgo aceptable para la empresa y aprueba el grado de madurez en seguridad global, habilitando los medios y recursos necesarios para su consecución.

3.4.3. Comprensión y concienciación

Considera las acciones formativas en materia de seguridad global impartidas a los directivos, responsables de los activos, miembros del equipo de seguridad y *stakeholders*.

3.4.4. Implantación del programa

Contempla la identificación de activos y los directivos responsables de los mismos. Analiza los riesgos y determina su impacto, documenta los riesgos y prioriza el nivel de protección en función de la criticidad del activo y de los riesgos que le pueden afectar.

3.4.5. Gestión y seguimiento del programa

Valora la revisión y actualización periódica de los planes de mitigación de riesgos. Los informes de situación, su periodicidad y la difusión de los mismos a los directivos responsables de los activos, al departamento de seguridad, así como al Comité de Dirección y Consejo de Administración de la empresa.

3.4.6. Alineamiento de la actividad de mitigación de riesgos de seguridad

Mide el grado de desarrollo y definición de funciones y responsabilidades, así como la monitorización y comunicación de las actividades de mitigación de riesgos y la gestión de incidentes.

Las auditorías y revisiones periódicas son fundamentales para verificar el estatus y grado de implantación del ESRM, de forma que se pueda

incorporar el proceso de mejora continua en la cultura de seguridad de la empresa. La valoración del nivel de madurez de la empresa no solamente calcula el *rating* global de la empresa en seguridad, sino que facilita una información precisa sobre cuál es el nivel que la empresa ha alcanzado en cada categoría y cuáles son las áreas de la organización que necesitan mejorar.

4. Modelo de Seguridad Global en una empresa multinacional de servicios esenciales

4.1. Introducción

Después de presentar dos modelos de referencia, para la gestión de riesgo de seguridad, vamos a compartir el caso práctico de implantación de un modelo de seguridad global en una empresa multinacional, del sector de la energía (electricidad y gas), operadora de servicios esenciales y con infraestructuras críticas en diferentes países, entre los que se incluyen zonas de alto riesgo. Gestiona un importante parque de centrales de generación eléctrica que incluyen todas las tecnologías: nuclear, térmica convencional (gas y carbón, esta última ya descatalogada), producción hidráulica, eólica y solar.

En el negocio de la distribución de electricidad se dispone de redes y líneas de distribución, subestaciones y centros de transformación. El negocio del gas cuenta con plantas regasificadoras, almacenamientos, gasoductos (algunos transnacionales) y estaciones de compresión. Tiene una presencia internacional en veinte países.

La empresa esta designada como operador crítico de servicios esenciales, de acuerdo con la normativa europea de protección de infraestructuras críticas. Es un ejemplo muy representativo de empresa operadora de infraestructuras críticas en los mercados de electricidad y de gas.

4.1.1. Evolución de la seguridad

La empresa históricamente ha dispuesto de un área de seguridad con responsabilidades fundamentalmente en el ámbito de la seguridad física. Protección de personas y activos frente a riesgos de carácter deliberado (delincuencia y terrorismo, principalmente).

Antes de la promulgación de las directivas europeas de protección de infraestructuras críticas y de seguridad de las redes y sistemas de información, la empresa disponía de un modelo de seguridad, referenciado en los requerimientos de la legislación española de seguridad privada y en la de

las buenas prácticas metodológicas de asociaciones internacionales prestigiosas, como ASIS International.

Una singularidad en este modelo lo constituían las centrales nucleares, pues con anterioridad a las Directivas europeas, tenía un tratamiento específico para la seguridad de las mismas. El Consejo de Seguridad Nuclear (CSN), máximo órgano regulador y supervisor de la operación de las centrales nucleares, aplicando estándares internacionales, tenía exigencias de seguridad física notablemente superiores a las establecidas para cualquier otro tipo de instalación de generación de electricidad. Requerían que cada central nuclear dispusiera de un Plan de Seguridad Física en el que se detallaran las zonas críticas de la instalación, un análisis de riesgos deliberados detallado y el conjunto de medidas establecidas para garantizar la prevención, protección y respuesta a incidentes de seguridad. El CSN, a través de su área de Seguridad Física y con la colaboración de la Secretaría de Estado de Seguridad, realiza la supervisión periódica del cumplimiento de las medidas implantadas, valora los incidentes producidos y las correspondientes medidas de mejora.

4.1.2. Percepción de la seguridad

Tradicionalmente en el mundo de la empresa, los recursos dedicados a seguridad han sido vistos como una fuente de gastos, que puede reducirse a voluntad en momentos de crisis. No es fácil demostrar el retorno de la inversión que se hace para proteger los activos del negocio.

A pesar de que todos los días en los medios vemos cómo riesgos de carácter deliberado y catastrófico afectan de forma creciente a las organizaciones, es difícil trasladar la necesidad de implementar un modelo sólido de seguridad global, eficiente y que sea sostenible en el tiempo.

En este contexto, el desarrollo de la legislación europea en materia de protección de infraestructuras críticas y su implantación en los Estados miembros, ha constituido un elemento fundamental para incorporar en las empresas operadoras de servicios esenciales un modelo de seguridad de referencia que no sea cuestionable por razones económicas.

4.1.3. De la seguridad física a la seguridad global

La evolución tecnológica, con el imparable proceso de digitalización de nuestra sociedad y la irrupción de nuevos riesgos digitales, geopolíticos y medioambientales durante los últimos veinte años, ha tenido un impacto sin precedentes en la seguridad de las empresas. Se ha evolucionado desde un enfoque en la protección física de bienes y activos, hacia nuevos ámbitos como la ciberseguridad, la gestión del fraude, el análisis de riesgos e inteligencia y la gestión de crisis y continuidad de negocio.

La función de seguridad ha pasado de ser un elemento meramente de protección, a convertirse en un facilitador de los distintos negocios de la empresa, independientemente de dónde desarrolle sus operaciones.

Este enfoque global de la seguridad ha permitido visibilizar, con claridad y consistencia, el importante aporte de valor que hace la seguridad a la propia empresa y por extensión al conjunto de la sociedad, asegurando la prestación de servicios esenciales.

El mundo empresarial es un ecosistema altamente competitivo y eficiente, en donde lo que no «aporta valor» de forma directa o indirecta, es rápidamente eliminado. En este contexto, el enfoque de Seguridad Global se ha posicionado como un área de alto valor añadido que se hace imprescindible para garantizar el funcionamiento de la empresa en un entorno de riesgos cada vez más vulnerable, incierto, complejo y ambiguo.

4.2. El Modelo de Seguridad Global empresarial

4.2.1. Misión

Crear y mantener condiciones de seguridad ajustadas a los objetivos corporativos, en el que las personas estén seguras, los bienes estén protegidos, los negocios puedan desarrollarse, se salvaguarde y fortalezca la reputación de la empresa y sean identificadas oportunidades para la mejora, captando valor para la organización.

Los ámbitos que se contemplan en un departamento de seguridad global son los siguientes:

4.2.2. Estrategia

Es el mecanismo de planificación a largo plazo de que dispone la empresa para alcanzar sus objetivos. Se aprueba por parte del Consejo de Administración y establece las líneas maestras que debe seguir la empresa para garantizar el crecimiento, rentabilidad y cumplimiento de los requerimientos regulatorios. La seguridad global es considerada como un elemento necesario para garantizar la consecución de los objetivos. El área de Seguridad Global debe tener una estrategia, aprobada por la dirección, que esté integrada y alineada con la estrategia general de la empresa.

La entrada en nuevos mercados internacionales, el desarrollo de nuevas áreas de negocio como son las energías renovables, el proceso de digitalización de los procesos empresariales, externalización de actividades *core* del negocio, o los requerimientos regulatorios de las administraciones competentes, son entre otros, elementos que deben ser considerados dentro de la estrategia de seguridad global.

Conocer de cerca y entender los requerimientos de los planes estratégicos y analizar con anticipación los riesgos a los que pueden estar expuestos, supone un punto necesario para desarrollar la estrategia de seguridad que debe contribuir al normal desarrollo de las líneas maestras marcadas por el Consejo de Administración de la empresa.

4.2.3. Gobierno

En un entorno regulatorio cada vez más complejo y exigente, se hace fundamental desarrollar capacidades de gobierno. Esto incluye la definición de la estrategia de seguridad global, su despliegue en políticas, planes, normas y procedimientos. En ellos se establecen las reglas que la organización, empleados, contratistas y *stakeholders* deben adoptar para garantizar un nivel adecuado de seguridad a través de la aplicación de una cultura de seguridad que desde unos principios generales se adapta a los distintos entornos de operación y riesgos en los que opera la empresa.

El área de gobierno de seguridad define e implanta las normas y procedimientos mediante programas de concienciación, formación y entrenamiento para crear una cultura de seguridad sólida y sostenible.

También establece la estructura organizativa en la que se definen las funciones y responsabilidades de todos los agentes internos y externos que son parte de del Modelo de Seguridad Global.

Por último, realiza la supervisión y verificación del grado de cumplimiento mediante ejercicios de simulación y auditorías que sirven para medir el nivel de madurez en seguridad, detectando los puntos problemáticos y estableciendo las acciones correctoras.

4.2.4. Análisis de riesgos e inteligencia

Es un área transversal a todos los ámbitos de la seguridad global. Analiza los riesgos de carácter deliberado (seguridad física, ciberseguridad, fraude) y catastróficos (geopolíticos, medioambientales), que pueden afectar a los activos de la empresa. Realiza la monitorización y alerta, especialmente en el ámbito digital, para la detección temprana de situaciones potenciales de riesgo. El análisis de riesgos en un elemento fundamental para valorar la vulnerabilidad de la organización, priorizar los activos a proteger y establecer las medidas de adecuación necesarias para incrementar el nivel de madurez en seguridad.

La inteligencia de seguridad es una de las áreas de más reciente incorporación al mundo de la seguridad global y una de las que tienen un mayor impacto. La capacidad de analizar las problemáticas, de valorar los impactos potenciales y consecuencias, es fundamental para que la empresa pueda

adecuar sus medios y recursos allí donde sea más necesario. Conocer los riesgos derivados de una alianza empresarial, la valoración de entornos geopolíticos y sociales complejos, la anticipación de posibles situaciones de riesgo y crisis, ofrecen a la dirección de la empresa unas capacidades muy valiosas para reducir los riesgos en el desarrollo del negocio.

4.2.5. Seguridad física

Contempla la protección de personas, con especial énfasis en ejecutivos y empleados que por el desempeño de su actividad están expuestos a especiales condiciones de riesgo. Incluye la seguridad de los empleados en viajes y el personal expatriado en entornos de alto riesgo. También se encarga de la protección de bienes como son centrales de generación de energía, subestaciones, líneas de transporte y distribución de electricidad, plantas regasificadoras, gasoductos, edificios, almacenes, entre otros.

4.2.6. Seguridad de la información y ciberseguridad

La irrupción de los ciberriesgos asociados a la digitalización de los procesos de negocio y la creciente y compleja regulación en la materia, ha hecho necesario incorporar la protección de las redes de comunicación, los sistemas de información y la protección de los datos, al perímetro de seguridad de la empresa. En las empresas energéticas es particularmente importante la protección de los sistemas de control industrial, por su impacto en la operación del sistema eléctrico. Las líneas de acción principales en ciberseguridad son la formación y entrenamiento de los empleados para que sepan detectar y actuar ante los ciberriesgos, la integración de la ciberseguridad en todos los procesos de negocios, proyectos y tecnologías, la implantación y gestión de capacidades para la prevención, protección, respuesta e investigación frente a los ciberataques y la creación de una potente red de apoyo mediante la colaboración público-privada con organizaciones referentes.

4.2.7. Protección contra el fraude

Una de las lacras de nuestra sociedad es el alto impacto que los hechos fraudulentos tienen en las cuentas de resultados de las empresas. Estas situaciones se producen tanto desde el punto de vista interno, con empleados propios, como desde el exterior, con clientes y suministradores, o en colusión de ambos. Este es uno de los ámbitos en los que se puede visibilizar y justificar con mayor claridad el retorno de la inversión realizada en seguridad. Conocer las bolsas de fraude en la organización, identificar los autores materiales, establecer procedimientos y herramientas para impedir o dificultar el fraude y poner a disposición de las autoridades competentes

a los infractores, supone un aporte de valor tangible muy apreciado por las direcciones de las empresas.

4.2.8. Gestión de crisis y continuidad de negocio

El sector energético y en particular la energía eléctrica, constituye uno de los elementos sistémicos que pueden impactar más gravemente en el funcionamiento de nuestra sociedad. Las empresas eléctricas y de gas, por la naturaleza de su actividad y el riesgo de sus operaciones, están preparadas para gestionar situaciones graves de contingencia. A pesar de ello, la frecuencia, virulencia y gravedad de escenarios de crisis, como los derivados de graves conflictos geopolíticos y sociales, desastres naturales y, sobre todo, los ciberriesgos, hacen necesario fortalecer la capacidad de resiliencia para gestionar estas crisis y garantizar la recuperación y la continuidad de negocio.

Estas capacidades incluyen la elaboración de planes de crisis y continuidad de negocio, la creación de Comités de Crisis y la formación y entrenamiento periódico de sus miembros para prepararlos ante situaciones críticas.

4.2.9. Normalización

Bajo este epígrafe se incluyen todo el conjunto de políticas, normas, procedimientos y planes que regulan la actividad de seguridad en la empresa. Tienen diferentes niveles, estratégico, táctico y operativo, que se implantan en todos los ámbitos de la organización. En esta arquitectura normativa, se establece el «qué, cómo, cuándo, quién y dónde», de manera que se regulan claramente los procesos de gestión de riesgos de seguridad.

- Política de seguridad global (nivel estratégico)
  Es el documento del máximo nivel en la empresa que da naturaleza jurídica, visibilidad y apoderamiento al área de seguridad global. En el mismo se recogen de forma clara y simplificada el conjunto de normas internas establecidas para regular el funcionamiento de la seguridad en la organización. Establece cuáles son las áreas de responsabilidad correspondientes al área de seguridad global y a las áreas de negocio, así como las personas y organizaciones implicadas en la misma. Esta firmada por el máximo responsable ejecutivo de la organización y es difundida en todos los ámbitos y niveles de la organización para público conocimiento y cumplimiento.
- Normas y procedimientos (nivel táctico)
  Desarrollan los distintos niveles establecidos en la política. Como ejemplo existen la Norma General de Protección de Infraestructuras Críticas, la Norma General de Ciberseguridad o la Norma General de Crisis, entre otras.

A su vez, estas normas se desarrollan en un conjunto detallado de procedimientos específicos en los que, por ejemplo y para el caso de la norma de ciberseguridad, se despliegan en procedimiento de acceso a los sistemas, procedimiento de comunicación de incidentes, procedimiento de análisis forense, etc.

Este cuerpo normativo, que aquí queda muy simplificado por cuestiones de espacio, es fundamental para construir el armazón sobre el que se soporta la función de seguridad global de forma homogénea e integrada. Sin una naturaleza jurídica aprobada por la dirección y convenientemente difundida y conocida por toda la organización, no es posible desarrollar adecuadamente la función de seguridad global.

- Planes de seguridad (nivel operativo)
  En los Planes se detallan los activos a proteger, como personas, bienes, información, reputación. Se analizan los riesgos que pueden afectarlos y el grado de vulnerabilidad existente. Se detallan las medidas, incluyendo personas con sus funciones y responsabilidades, procedimientos operativos (control de accesos, vigilancia perimetral, acción frente a incidentes deliberados, monitorización desde el Centro de Operación de Seguridad, entre otros) y se establecen los medios técnicos pasivos (puertas, barreras, vallas, muros) y activo (detectores, controles de acceso, videovigilancia, entre otros).

  Los planes generales establecen las líneas operativas principales para toda la empresa, por ejemplo, el Plan de Seguridad del Operador (PSO), requerimiento de la administración competente para las empresas operadoras de servicios esenciales con infraestructuras críticas. Otro ejemplo es el Plan de Crisis Corporativo, que aplica a toda la organización en caso de una situación catastrófica, como concurrió con la epidemia del COVID-19.

  Los Planes de Protección Específicos (PPE) se refieren a la protección de un activo (una instalación o un servicio concreto). En el mismo se detallan los aspectos anteriormente mencionados, centrados en una instalación como puede ser el Plan de Protección Especifico de una Central Nuclear o el Plan de Continuidad de Negocio de zona geográfica de distribución de electricidad.

  Estos planes se vinculan entre sí dentro de la empresa y también se asocian con planes de otros organismos externos, como son los Planes de Acción Operativa de las Fuerzas y Cuerpos de Seguridad para la protección de infraestructuras críticas, o los Planes de Crisis vinculados con los Planes de Protección Civil de las diferentes poblaciones y comunidades autónomas. Estos planes son revisados y actualizados periódicamente.

4.2.10. Organigrama

La función de Seguridad Global, por su relevancia creciente, debe estar posicionada dentro del Comité de Dirección, de forma que esté cerca de la toma de decisiones y pueda ejercer su labor con el máximo apoyo de la dirección.

En este apartado se detallan las posiciones que deben formar parte de una organización de Seguridad Global, con sus funciones y responsabilidades.

- Director de seguridad global
  Es el máximo responsable de seguridad de la empresa. Su función es establecer la estrategia de seguridad; desarrollar e implantar el modelo de seguridad; seleccionar, organizar y gestionar el equipo humano del departamento, tanto en el ámbito funcional como territorial; obtener recursos de la organización para el desarrollo de las funciones encomendadas; planificar los objetivos y líneas de acción del ámbito de su competencia; dirigir la gestión de incidentes de seguridad y situaciones de crisis, aprendiendo y compartiendo las lecciones aprendidas; supervisar el cumplimiento de las medidas de seguridad que se determinen; informar periódicamente a la dirección y al Consejo de Administración de los avances en la mejora de la seguridad, así como de los principales incidentes y, por último, actúa como máximo representante de la empresa ante los organismos e instituciones de seguridad públicos y privados. En concreto, actúa como responsable de Seguridad y Enlace, frente a las autoridades competentes, de acuerdo con el Modelo PIC.

- Responsables funcionales de seguridad
  Se establecen por cada una de las áreas de especialización: gobierno de seguridad, seguridad física, seguridad de la información y ciberseguridad (que a su vez actúa como responsable de Seguridad de la Información con las autoridades competentes), análisis de riesgo e inteligencia, protección contra el fraude y resiliencia, crisis y continuidad de negocio. Cada uno de ellos es el máximo especialista en su materia y responsable de analizar los riesgos, determinar las medidas más adecuadas para su control, mitigación y gestionar los incidentes graves del ámbito de su competencia, al igual que supervisar y velar por el cumplimiento de las medidas de su ámbito en el conjunto de la empresa. Representan a la dirección de seguridad en los organismos y foros públicos y privados para realizar el intercambio de información y experiencias con el objeto de fortalecer las capacidades colaborativas de la organización.

- Responsables de seguridad operativos
  Gestionan la seguridad global en un determinado territorio o geografía. Realizan la implantación de medidas técnicas y la operación de los diferentes servicios de seguridad de todas las áreas funcionales en su ámbito

de competencia. Representan a la empresa en aquellos organismos públicos y privados que sean necesarios para el ejercicio oportuno de su actividad. Proponen a los delegados de Seguridad de las infraestructuras críticas. Gestionan los incidentes de seguridad global en su ámbito y se apoyan para ello en los responsables funcionales o en el apoyo experto que se considere necesario. Dependen de la dirección de seguridad y prestan servicio a las áreas de negocio de la empresa. De esta forma, se garantiza la independencia y el tratamiento homogéneo de la seguridad en todo el ámbito de la empresa.

4.2.11. Órganos de gobierno y coordinación

Para realizar una adecuada integración y gestión de la seguridad global en la empresa, es necesario establecer mecanismos de coordinación formales internos y externos como los que se detallan a continuación:

- Comité de seguridad global
  Es el máximo órgano de gobierno de la seguridad. Está compuesto por directivos representantes de las áreas de negocio y áreas corporativas. Lo preside el directivo de mayor rango, actuando como secretario el director de Seguridad.

  En el comité se aprueban las estrategias y los planes de acción con la consiguiente dotación de recursos. Se reúne con periodicidad trimestral o cuando una situación grave lo requiera.

  El área de seguridad reporta periódicamente el grado de avance de los objetivos marcados, presenta un Mapa de Madurez en el que se refleja el estado de seguridad e informa de todos los incidentes relevantes acontecidos en el periodo, con las consecuencias y lecciones aprendidas. Con una periodicidad cuatrimestral, el comité aprueba un informe de situación que se presenta al Consejo de Administración, para informar al máximo órgano de gobierno de la empresa sobre el estado, evolución de las condiciones de seguridad e incidentes relevantes.

  Este comité a su vez se desglosa en otros subcomités específicos como son el de Protección de Infraestructuras Críticas, el de Ciberseguridad, el de Protección contra el Fraude o el de Resiliencia. En los mismos la estructura organizativa y miembros es similar al Comité de Seguridad Global, con representantes de las diferentes unidades de la empresa, pero los temas tratados son de nivel táctico-operativo. Esta estructura permite garantizar la interacción de forma transversal con todas las unidades de forma transparente y facilita su implicación y compromiso para la dotación de recursos, implantación y mantenimiento de las medidas adoptadas.

- Comités de coordinación con organismos externos
  Con el fin de facilitar el intercambio de información sobre lecciones aprendidas de incidentes, mejores prácticas y de establecer mecanismos de ayuda mutua en caso de incidentes graves, se promueve la participación en foros y grupos de trabajo interdisciplinares que permitan contribuir de forma significativa a la mejora de las capacidades de prevención, protección, respuesta y recuperación.

  De estos destaca el Comité de Protección de Infraestructuras Críticas, liderado por el CNPIC, que sirve de punto de encuentro entre las diferentes administraciones públicas competentes y los responsables de Seguridad y Enlace y los responsables de Seguridad de la Información de los operadores de servicios esenciales.

5. Conclusiones

El mundo de la seguridad ha evolucionado muy rápido en los últimos años, consecuencia de la irrupción de riesgos digitales, geopolíticos y medioambientales, que crean escenarios cada vez más complicados e inestables para la empresa.

A la proliferación y gravedad de estos riesgos, se suma un contexto regulatorio más exigente, en particular para entidades que prestan servicios esenciales.

Este entorno ha llevado a que las empresas hayan desarrollado nuevos Modelos de Seguridad Global, que, desde una perspectiva integrada, eficiente y sostenible, sean un apoyo, cada vez más importante, para conseguir los objetivos de negocio.

A continuación, se detallan algunos de los elementos más relevantes de este nuevo enfoque en el Modelo de Seguridad Global:

- Catalogación de los activos de la empresa, en función de su importancia e impacto para el negocio y para la sociedad, para priorizar su protección.
- Visión holística de todos los riesgos de seguridad, físicos, digitales, fraudes y catastróficos, de forma que se pueda hacer una gestión global y homogénea de los mismos.
- Desarrollo de una estrategia de Seguridad Global, que establezca los objetivos y líneas de acción principales del área de seguridad, alineada con la estrategia general de la empresa.
- Establecimiento de mecanismos de gobierno, como el Comité de Seguridad Global, que facilite la toma de decisiones, coordinación y supervisión de la gestión de la seguridad, así como el reporte a los niveles de dirección de la empresa.

- Corresponsabilización de los responsables de las unidades de negocio, conjuntamente con el equipo de seguridad global, para identificar los riesgos de seguridad, priorizarlos en función de su impacto y realizar una gestión conjunta de los mismos.
- Colaboración público-privada y privada-privada en el desarrollo y gestión de modelos de seguridad que comprometan a todas las partes involucradas, como son las Administraciones públicas y las empresas, en la mejora de las condiciones de seguridad de nuestra sociedad.
- Extensión del modelo de seguridad global a los proveedores que forman parte de la cadena de suministro, en particular los relacionados con las redes y sistemas de información.
- Desarrollo de las capacidades de inteligencia de seguridad para anticipar situaciones de riesgo emergentes, en particular en el mundo digital.
- Preparar y entrenar a las diferentes áreas de negocio para afrontar incidentes graves y situaciones de crisis, mediante el fortalecimiento de las capacidades de resiliencia, como son la gestión de incidentes y situaciones de crisis y los planes de continuidad de negocio.

Composición del grupo de trabajo

Presidente: **D. Luis Alberto Hernández García**
Coronel del Ejército de Aire y del Espacio
Jefe de la Sección de Análisis y Prospectiva del Estado Mayor Conjunto

Secretario: **D. Fernando Riaño Echanove**
Capitán de fragata de la Armada
Analista de la Sección de Doctrina del Estado Mayor Conjunto

Autores: **D. Casildo Luis Martínez Vázquez**
Coronel del Ejército del Aire y del Espacio
Agrupación del Cuartel General del Ejército del Aire y del Espacio

D. Claudio Sánchez Sánchez
Coronel del Ejército de Tierra
Jefe de la Jefatura de Adiestramiento y Doctrina de Infantería de la Dirección de Doctrina, Orgánica y Materiales del Ejército de Tierra

D. Alberto Cique Moya
Coronel veterinario del Cuerpo Militar de Sanidad
Jefe de la Sección de Análisis de la Jefatura Conjunta de Sanidad del Estado Mayor Conjunto

D. José Ángel Tortosa Delfa
Capitán de fragata de la Armada
Joint Effects Branch Head. NATO Joint Force Command Norfolk

D. José Luis Bolaños Ventosa
Senior Advisor Global Security

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL