MINISTERIO DE DEFENSA

ESTADO MAYOR DE LA DEFENSA

CONCEPTO DE CIBERDEFENSA

RESUMEN EJECUTIVO

CESEDEN
CENTRO CONJUNTO DE DESARROLLO DE CONCEPTOS
PASEO DE LA CASTELLANA 61
28 DE SETIEMBRE DE 2018

[REVERSO DE PORTADA]

A MODO DE PRESENTACIÓN

El ciberespacio es un entorno global en constante evolución, donde la amenaza es cada vez más activa y sofisticada (actores estatales, terroristas, criminales, etc…), amenaza que puede poner en riesgo no solo redes y sistemas de información y telecomunicaciones del Ministerio de Defensa y las Fuerzas Armadas, sino también las infraestructuras críticas y servicios esenciales de España, o incluso atentar contra la propia estabilidad nacional.

Es necesario, por tanto que las Fuerzas Armadas (FAS), y el Ministerio de Defensa (MDEF) en general, de una respuesta global e integral a este importante desafío.

Para ello y partiendo del análisis del entorno operativo actual y del previsible futuro, el Centro Conjunto de desarrollo de Conceptos (CCDC), con la participación de expertos de los diferentes organismos implicados del MDEF, y siguiendo la metodología de Desarrollo de Conceptos y Experimentación (CD&E), ha desarrollado el Concepto de Ciberdefensa, concepto que está alineado con las iniciativas desarrolladas en este campo tanto en el ámbito nacional, como en el internacional.

El Concepto que hoy se presenta, aborda de forma global e integral todos los campos operativos de la Ciberdefensa, con una terminología común, una definición clara de sus capacidades, la necesaria coordinación con los actores que operan en el ciberespacio y en el espectro electromagnético, las operaciones militares en el ámbito del ciberespacio y su integración con el resto de capacidades operativas, así como su estructura de Mando y Control (C2), el marco legal de actuación y la imprescindible integración con el resto de actores civiles y militares a nivel nacional e internacional; y todo ello para orientar **el desarrollo de las capacidades necesarias para enfrentar la amenaza de hoy y del mañana**.

1. ANTECEDENTES

Ya en el año 2011 el entonces Jefe del Estado Mayor de la Defensa (JEMAD) abordó el problema de la Ciberdefensa para dar una serie de orientaciones y establecer el marco de referencia para el desarrollo y empleo de las capacidades militares en el ciberespacio.

Pero como se decía en la presentación el mundo cambiante y rápido en el que vivimos, y la evolución constante de las nuevas tecnologías ha hecho imprescindible revisar la Doctrina y las capacidades de Ciberdefensa de nuestras FAS; entre estos cambios se encuentran la publicación de las *Estrategias de Seguridad Nacional* (2013 y 2017) y de la *Estrategia de Ciberseguridad Nacional* de 2013; la creación del *Mando Conjunto de Ciberdefensa* (MCCD, 2013) y del Centro de Sistemas y Tecnologías de la Información y las Comunicaciones (CESTIC, 2015); la publicación por parte del SEDEF de la nueva política de Sistemas y Tecnologías de Información y Comunicaciones (CIS/TIC) (2015), de la Arquitectura Global CIS/TIC del MDEF (2016) entre otros, y el nuevo *Concepto de Empleo de las FAS* del JEMAD (2018) que destaca «*la importancia del ciberespacio como un nuevo ámbito de seguridad*».

2. OBJETO

El concepto liderado por el CCDC busca proporcionar el ***marco conceptual*** que sirva de orientación para el proceso de implementación de las capacidades de Ciberdefensa dentro del ciclo de *Planeamiento de la Defensa,* así como establecer los **principios fundamentales** que deben guiar el posterior ***desarrollo doctrinal*** para este nuevo ámbito de las operaciones militares.

3. ALCANCE

Partiendo del análisis del entorno operativo actual y del previsible futuro, el Concepto aborda de forma global todos los ámbitos de la Ciberdefensa. Presenta una terminología común, una definición clara de las capacidades (defensa, explotación y ataque), las operaciones militares en el ámbito del ciberespacio y su integración en las de operaciones militares conjuntas, el marco legal de actuación, la estructura de C2 y la necesaria integración con el resto de actores en el marco de las actuales políticas en materia CIS/TIC y SEGINFO[1] dentro del proceso de transformación digital que afecta a la totalidad del MDEF. Asimismo, presenta consideraciones sobre Investigación Desarrollo e innovación (I+D+i), materiales, concienciación, enseñanza, adiestramiento y personal.

4. RETO OPERATIVO

El entorno operativo actual, así como el previsible entorno futuro y las implicaciones que de él se derivan para las capacidades de las FAS, y del MDEF en general, constituyen la base sobre la que se fundamenta este Concepto.

En este sentido consideramos el ciberespacio:

- un entorno global y dinámico, en constante evolución;
- un escenario complejo con características propias que favorecen la actuación del atacante (bajo coste relativo, fácil acceso y ejecución, ubicuidad, gran efectividad e

[1] SEGINFO: Seguridad de la Información

impacto, con un marco legal dispar y difuso, y reducido riesgo dado el anonimato y la difícil atribución);

- un nuevo ámbito de las operaciones militares[2], cada vez más relevante;
- un ámbito ligado al espectro electromagnético y transversal al resto de ámbitos físicos y cognitivo, en el que las acciones que se realizan en él pueden causar importantes efectos sobre el resto de ámbitos (incluso daño físico sobre sistemas, equipos, personas, etc.);
- un entorno en el que existen amenazas permanentes cada vez más sofisticadas provenientes de actores diversos (actores estatales, grupos terroristas, crimen organizado, hacktivistas, etc.) que comparten el mundo civil y militar, el ámbito nacional e internacional;
- un ámbito desde el cual se puede poner en riesgo el correcto funcionamiento de los organismos del MDEF, la capacidad de operar de las FAS, o atentar contra las infraestructuras críticas y servicios esenciales de un país o contra la propia estabilidad nacional.

El terrorismo y las **ciberamenazas** suponen uno de los retos más importantes para la Seguridad Nacional. Las ***«acciones híbridas»*** que combinan las clásicas acciones militares convencionales con otras no convencionales, como los ciberataques, operaciones de manipulación de la información u otros elementos de presión, política, social o económica, son una realidad en el escenario actual y lo seguirán siendo en el previsible escenario futuro.

En este contexto, las FAS, y el MDEF en general, se encuentran ante el reto de potenciar sus actuales capacidades de Ciberdefensa para:

- fortalecer la resiliencia,
- operar de forma continuada, ágil y eficaz en el cada vez más exigente escenario operativo
- y ser capaces de evolucionar y adaptarse al ritmo que lo hacen las tecnologías y la propia amenaza;

Todo ello, garantizando en todo momento la legalidad y legitimidad de sus acciones y operando en colaboración y coordinación permanente con el resto de actores civiles y militares del ámbito nacional e internacional, según los acuerdos vigentes en cada caso.

[2] "*At the Warsaw Summit (2016), they reaffirmed NATO's defensive mandate, pledged to enhance the cyber defences of their national networks and infrastructures, and* ***recognized cyberspace as a domain of military operations, in which NATO must defend itself as effectively as it does in the air, on land, and at sea"*** *NATO 2018.*

5. IDEA CENTRAL: «INTEGRACIÓN»

Se considera imprescindible dar una respuesta global e integral para el conjunto de las FAS, y para el MDEF en general, en línea con el desarrollo de las vigentes políticas del departamento y en estrecha coordinación con los organismos responsables de la provisión de servicios y en la operación y mantenimiento de redes y sistemas, que permita hacer frente de forma eficaz a los importantes desafíos que se afrontan en este ámbito.

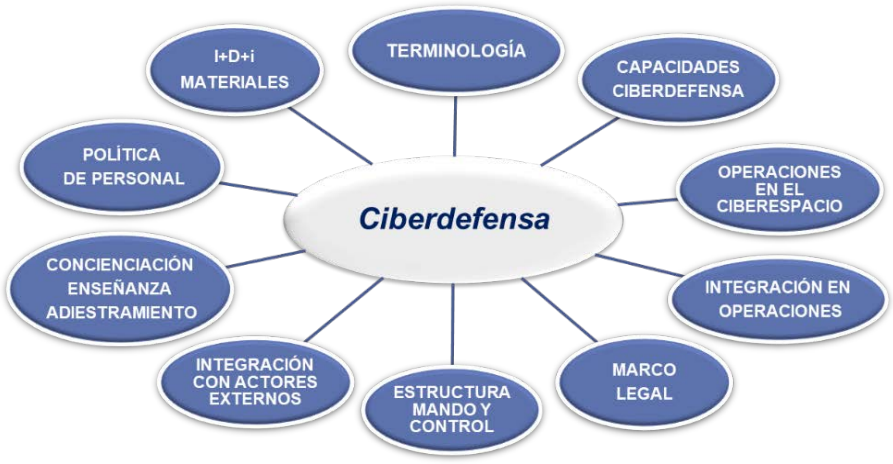
La Ciberdefensa como capacidad militar, debe estar plenamente integrada en todos los ámbitos dela s FAS, y del MDEF en general, así como con el resto de actores civiles y militares del ámbito nacional e internacional con quienes compartimos riesgos y amenazas.

Por otro lado se considera el factor humano como clave del éxito, referidos no solo al personal técnico y operativo involucrado en las actividades del ciberespacio, sino todo personal usuario de los servicios que se proporcionan a través de las redes y sistemas.

6. ELEMENTOS PARA UN A SOLUCION

Los ***elementos centrales de una solución*** que permita dar respuesta eficaz al *reto operativo* que afronta el MDEF, y las FAS en particular, se encuentran en:

(1) La necesidad de contar con una *Terminología Común*.
(2) La definición clara de las *Capacidades de Ciberdefensa*.
(3) Las Operaciones militares en el ámbito del ciberespacio.
(4) La *Integración de las capacidades de Ciberdefensa* en las operaciones militares conjuntas.
(5) El *marco legal* de actuación y políticas CIS/TIC y SEGINFO en el MDEF.
(6) Una *Estructura de Mando y Control* clara, ágil y eficaz, en la que estén integrados todos los medios con los que cuenta el MDEF y las FAS en particular.
(7) La Integración con otros actores civiles y militares del ámbito nacional e internacional.
(8) Las medidas específicas a adoptar en materia de *Concienciación, Enseñanza y Adiestramiento* del personal.
(9) Las consideraciones sobre *Personal, en lo referente a este concepto*.
(10) Las consideraciones específicas sobre *I+D+i y en el campo de los Recursos Materiales*.



7. CONCLUSION.

El concepto de Ciberdefensa desarrollado por el CCDC y aprobado por el JEMAD proporciona una guía para afrontar el desarrollo de capacidades militares y la organización de las FAS en el ámbito del ciberespacio que deberá ser desarrollada con mayor profundidad durante la *Fase de Implementación* de este Concepto y podría suponer la revisión de determinadas políticas y normativa del MDEF actualmente en vigor. Todo ello para habilitar a nuestras Fuerzas Armadas frente a una amenaza emergente y en constante evolución, y garantizar así la defensa de los intereses nacionales allá donde se nos requiera.