Futuro de la Ciberdefensa en las FAS y perfil de carrera para su personal

Autor: Santos Sande, Carlos Alberto

Director: Rodríguez Rodríguez, Francisco Javier.

Contacto: csansan@fn.mde.es

Resumen: Las Operaciones en el Ciberespacio son parte del ámbito operativo más moderno dentro de nuestras Fuerzas Armadas. Así, a raíz de esta necesidad se creó *el Mando Conjunto de Ciberdefensa* el 19 de febrero de 2013. Después de casi siete años de andadura se considera necesario estudiar cual puede ser su futuro al que inexorablemente va unido el perfil de carrera de su personal. En este contexto, el presente TFM plantea la necesidad de aunar bajo un mismo mando operativo, en este caso el JEMAD, todo lo relacionado con el mundo CIS y el de Ciberdefensa. Se propone la creación de un mando único, el *Mando Conjunto del Ciberespacio*, que se encargue de proveer los servicios CIS, así como un *responsable* de su ciberdefensa, con la finalidad de solventar las disfunciones operativas existentes en la actualidad.

El nuevo *Mando Conjunto del Ciberespacio* precisaría de profesionales formados y adiestrados, capacitados para su continua adaptación a la amenaza existente. Este personal operativo precisa de una continuidad en este ámbito, pues el "know-how" y el "expertise" indispensable para combatir a los actores hostiles se alcanzan con un esfuerzo continuo y una dedicación permanente. Actualmente, el perfil de los Ejércitos y Armada no valora este perfil de carrera, imprescindible para combatir en el ciberespacio. Esta es la razón por la que se propone, a corto-medio plazo, la creación de un *Cuerpo Común del Ciberespacio*, y, a medio-largo plazo, una nueva rama en las FAS, el *Ejército del Ciberespacio*.

Palabras clave: Ciberespacio, independencia, ciberguerrero, Ejército, talento, Employer Branding.

---

1. Introducción

1.1. Motivación

A lo largo de ya más de cuatro años en el MCCD he tenido la oportunidad de apreciar las virtudes y las carencias que posee esta Unidad para convertirse en una unidad de combate dentro de las FAS españolas. Esta Unidad debería convertirse en el punto de referencia en todos los factores condicionantes relacionados con la ciberdefensa, la ciberseguridad y la ciberinteligencia, tanto para las Administraciones Públicas como para? el entorno empresarial. Las FAS en muchos ámbitos en los que desarrollan sus capacidades deberían ser, y en muchos casos son, un referente para otras administraciones y para el sector empresarial, como así sucede en otros países de nuestro entorno, pero en especial deberían de serlo en el ámbito del ciberespacio. El MINISDEF debería de potenciar y respaldar al MCCD en diversos campos, tal y como se refleja a lo largo del presente TFM, si se quiere que este Mando tenga la capacidad de enfrentarse a los potenciales enemigos que afectan tanto a las FAS como a la Seguridad Nacional en el ciberespacio.

El campo de batalla del ciberespacio es completamente transgresor con respecto a los tradicionales Tierra, Mar y Aire y, en línea con ello, su personal tiene que estar dotado de unas cualidades profesionales y unas características personales diferenciadas de las requeridas y valoradas en la actualidad por los Ejércitos y Armada. En este sentido, estas razones originan que en este trabajo se elaborarán y detallarán propuestas para conseguir que el dominio de las operaciones en el ciberespacio resulte altamente operativo; consiguiendo, a su vez, la captación, retención y motivación del personal operativo en esta joven área de las operaciones militares.

1.2. Objetivos

Los objetivos del presente trabajo claramente son dos: por un lado, y partiendo de la situación actual del MCCD, evaluar hacia donde debe dirigirse este Mando tanto orgánica, estructural como operativamente y, por el otro, basándonos en la situación de su personal, analizar cómo debe ser el perfil de carrera hacia el que se debe tender, a diferencia del que existente en la actualidad, para conseguir motivación, se encuentre un elevado grado de captación y, sobre todo, de retención. Se pretenden definir posibles soluciones para disponer de una trayectoria profesional en este ámbito de las operaciones, que permitan conjugar, adecuada y eficientemente, la formación en Ciberdefensa, la experiencia que se debe adquirir en el destino y las aspiraciones profesionales de sus miembros.

La finalidad reside en definir una estructura y marcar un futuro para la Ciberdefensa dentro de las FAS, de modo que ésta sea una plataforma de desarrollo profesional para sus miembros; consiguiendo, con ello, elevar la operatividad y colocar la labor que realiza este Mando en los niveles de excelencia necesarios para situarse como un centro de referencia en este entorno, tanto a nivel militar como civil, y en la esfera nacional e internacional.

2. Desarrollo

Este TFM expone la situación actual de la Ciberdefensa dentro de las FAS y cómo es el perfil de carrera de su personal. Partiendo de este punto, se propone una línea de acción que debería seguir la Ciberdefensa con la intención de tener un futuro operativo y ser la cabeza de lanza en los futuros campos de batalla en los que intervengan las FAS; los cuales, dado que serán cada vez menos

convencionales, obligarán la mayor parte del tiempo a combatir en la conocida como *Zona Gris*[1]. Por ende, las necesidades específicas de su personal para poder llevar a cabo la misión se diferenciarán de las actualmente demandadas por nuestras FAS.

2.1. Presente y futuro de la Ciberdefensa en las FAS.

El dominio ciberespacial se define como el dominio global virtual compuesto tanto por las redes interconectadas como por las redes y sistemas aislados o independientes [2]. En base a esta definición el mundo CIS y el de la Ciberdefensa deben ir íntimamente unidos. Al comenzar el presente TFM existían tres actores en esta esfera operacional: el CESTIC, la JCISFAS y el MCCD. Los cuales estaban en dos cadenas de mando bien diferenciadas: el CESTIC, como proveedor de servicios CIS, dependiente del SEDEF y la JCISFAS y el MCCD del JEMAD. A finales de 2020, la JCISFAS y el MCCD se integraron en un único Mando: el Mando Conjunto del Ciberespacio (MCCE).

En este trabajo se propone que el primer paso para el futuro de la Ciberdefensa en las FAS resida en la integración de las tres unidades en una sola, el MCCE, bajo dependencia operativa del JEMAD, responsable de las operaciones; siendo este Mando el asesor estratégico en materia de ciberdefensa del JEMAD.

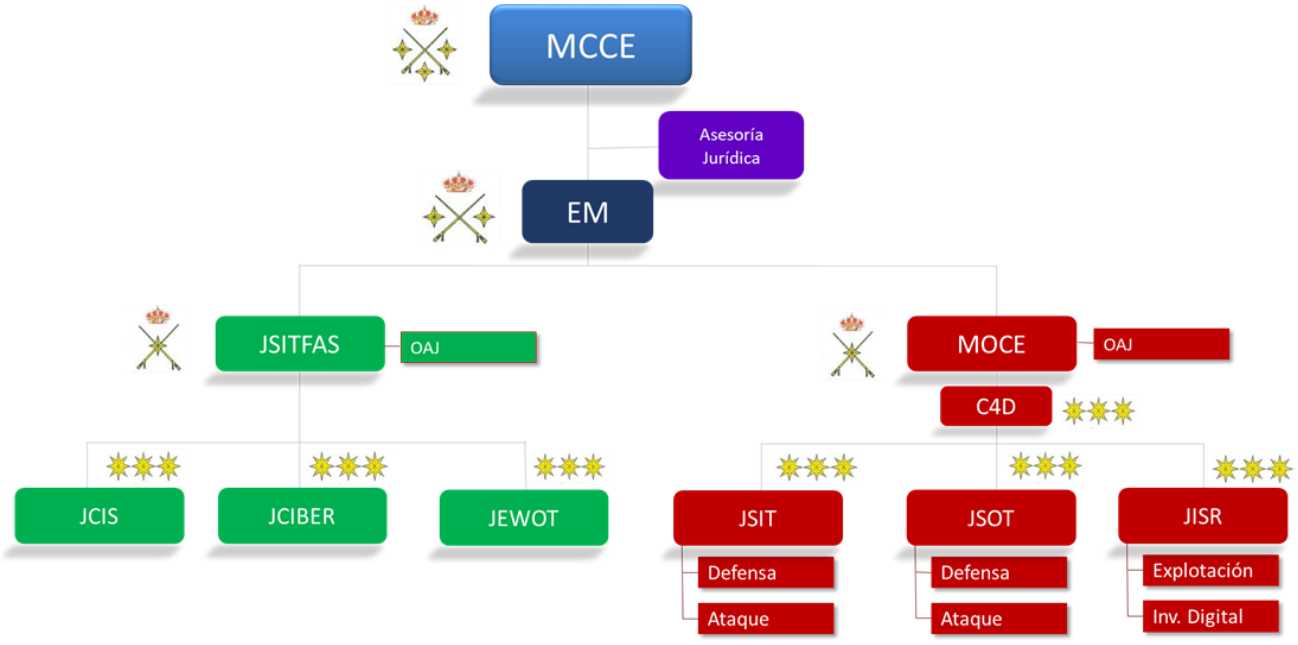

Figura 1. Estructura orgánica del MCCE (elaboración propia)

Debajo del MCCE deben colgar dos estructuras diferenciadas: la *Jefatura de Sistemas y Tecnologías de las FAS (JSITFAS)* y el *Mando de Operaciones en el Ciberespacio (MOCE)*. En este sentido, en relación con los responsables de los sistemas y los encargados de su ciberdefensa, no se considera operativo que estas Unidades deban de pertenecer a dos entes separados ni a dos cadenas de

[1] "Existe una zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe entre estados (bona fide) que pese a alterar notablemente la paz no cruzan los umbrales que permitirían o exigirían una respuesta armada. Es la llamada zona gris.

Las actividades que se pueden llevar a cabo en esta zona, entre las que se encuentran los ciberataques, la propaganda, los sabotajes, las operaciones encubiertas o clandestinas, los disturbios y otras similares, tienden a mantenerse en un entorno de baja intensidad. Dichas actividades, con mayor o menor grado de ambigüedad y visibilidad, persiguen crear un clima de desinformación y confusión que desestabilicen y debiliten al adversario."[1]

mando distintas, como pasa en la actualidad con el MCCE y el CESTIC. EL CMCCE deberá aportar directrices y asignar misiones y responsabilidades a cada una de sus jefaturas subordinadas, pero estando ambas dentro de la misma estructura orgánica, bajo una única dirección y subordinadas a la cadena operativa e integrada en la FC. Por tanto, la JSITFAS será el proveedor de servicios CIS de las FAS y el MOCE dispondrá de las capacidades militares de Defensa, Explotación y Ataque para poder liderar y llevar a cabo las operaciones en el ciberespacio.

2.2. Presente y futuro del perfil de carrera del personal de Ciberdefensa.

En la actualidad, en las FAS no existe un perfil específico de ciberdefensa, por lo que el personal que desarrolla su labor profesional en este ámbito de las operaciones es valorado acorde a los criterios de evaluación de cada uno de sus ejércitos de procedencia, teniendo en consideración cualidades o perfiles específicos orientados a las necesidades de cada uno de ellos, no teniendo en valor la labor realizada tanto en el MCCD como en las Unidades de Ciberdefensa propias de los Ejércitos y Armada. En los Ejércitos y Armada se valora la rotación en diversos destinos de su personal y, en el caso de los oficiales, hacer mando en alguna de sus unidades operativas. Las peculiaridades de las necesidades del perfil de carrera del personal del ciberespacio implican penalización a la hora de ser evaluado para el ascenso y no truncar su carrera profesional dentro de su propio ejército.

En el TFM se aportan propuestas con el fin de conseguir que la permanencia en el área de las operaciones en el ciberespacio no penalice al personal que quiera hacer carrera en ella. Se considera que la única forma de conseguir este fin es que el personal se desligue de su ejército de procedencia, para lo cual se indican dos propuestas, una a corto-medio plazo y otra a medio-largo plazo. La primera propuesta es la creación de un *Cuerpo Común del Ciberespacio*, para conseguir la permanencia de su personal altamente cualificado y adiestrado, pues de lo contrario será imposible conseguir una masa crítica de personal capacitado y especializado en este ámbito. Esta posibilidad es factible al existir ya la estructura orgánica de los Cuerpos Comunes, de modo que debería de crearse un nuevo cuerpo para oficiales y suboficiales. La segunda propuesta focaliza la atención en la creación del Ejército del Ciberespacio como una rama independiente como el Ejército de Tierra, la Armada y el Ejército del Aire.

Una vez abordados los aspectos anteriores se plantean diversas formas de reclutar personal para cubrir sus necesidades específicas y que desempeñe su labor en este ámbito de las operaciones:

a) Dentro de las FAS: no se considera que deba existir una academia específica para formar al personal de la Fuerza desde el comienzo de su trayectoria profesional. La propuesta que el presente TFM aporta establece que los oficiales y suboficiales deben cumplir servidumbre en sus ejércitos de procedencia en el primer empleo y parte del segundo, con la finalidad de que adquieran las capacidades de liderazgo y gestión del estrés.

   Se propone seguir el modelo de la Armada en la especialización complementaria para oficiales. En el segundo año del segundo empleo (respecto a oficiales y suboficiales) se ofertarán plazas de especialización en el ámbito del ciberespacio a personal de los Ejércitos y Armada.

b) Captación de talento fuera de las FAS: se propone crear una Comunidad del Ciberespacio que posea una estrecha relación con otras instituciones, centros de formación y empresas relacionadas con los sistemas y redes de comunicaciones, la ciberseguridad y la ciberinteligencia, que servirá como fuente para la captación de personal para trabajar en el

MCCE basándose en su *Marca de Empleador* o "*Employer Branding*". Se considera necesario fomentar la imagen del MCCE para atraer a personal civil cualificado en su primera etapa profesional.

Se proponen tres formas de rejuvenecer el MCCE y captar e integrar el talento en este ámbito: captar trabajadores que se integren como personal de complemento, contratar personal civil recién titulado universitario y de centros de formación profesional y la activación de reservistas voluntarios en las escalas de oficiales y suboficiales.

La oferta de plazas para militares de complemento conseguirá cubrir el déficit de oficiales y suboficiales en los primeros empleos militares y permitirá crear una masa crítica de personal técnico en la base de la pirámide organizacional.

Además, se considera necesario focalizar la atención en el reclutamiento a medio plazo, el cual podría abordarse mediante la creación de becas formativas financiadas por el MINISDEF, por medio de las cuales se asumiría la realización de un título universitario o de formación profesional. Una vez finalizada la formación se vincularía el beneficiario a las FAS con un contrato temporal, como es el caso de los militares de complemento.

Una de las principales ventajas derivadas de esta variedad de formas de ingreso reside en la posibilidad de atraer talento sin necesidad de que vistan el uniforme militar, lo cual es un signo diferenciador y una ventaja competitiva con el resto de las FAS.

Mientras no se consiga llevar a cabo la creación de una rama específica del Ciberespacio, ya sea Cuerpo Común o Ejército, que asegure un perfil de carrera propio para su personal, se tienen que valorar otras alternativas para incrementar el atractivo de cara a la captación y, especialmente, a la permanencia del personal dentro de este ámbito, en el MCCE o las Unidades de Ciberdefensa de los Ejércitos y Armada. En este sentido, los aspectos en los que se puede enfocar el Mando para mejorar la retención son los siguientes:

a) Valoración del destino: la solución para que el MCCE posea un elevado porcentaje de cobertura de su plantilla, mientras no se cree una rama específica del ciberespacio, es que los Ejércitos y Armada consideren como una unidad de Fuerza tanto al MCCE como a las unidades específicas de Ciberdefensa de los Ejércitos y Armada.

   Los oficiales del MCCE para avanzar en su carrera profesional, en determinados momentos de la misma, han de ejercer Mando de Unidad. Con la finalidad de retener personal adiestrado para combatir en el ciberespacio, actualmente un bien escaso que afecta su desembarco en la operatividad de la unidad, se propone que ciertos destinos dentro de la FOCE o el EM sean considerados como si estuvieran ejerciendo el Mando en unidades operativas.

b) Informes Personales de Calificación (IPEC): los IPECs en el MCCE son superiores a la media, pues su personal está muy especializado, altamente cualificado y realiza su trabajo con un elevado grado de precisión y calidad. No obstante, al depender de los Ejércitos y Armada su ponderación, resulta difícil encontrar un punto de mejora en esta área.

La diferencia de valoración de los IPECs se convierte en un punto más a favor de la creación a corto plazo del C.C. del Ciberespacio, en el cual todos sus profesionales serían valorados por los criterios de una sola institución.

c) Medallas: se propone crear y promover dos tipos de medallas:

   - La medalla específica al "*Mérito ciberespacial*", que implicaría disponer de una condecoración diferenciadora que premiase la labor realizada en el ciberespacio, y así valorar al mismo nivel los méritos acreditados en cada uno de los ámbitos de las operaciones.

   - La "*Medalla de Operaciones Permanentes*" realizadas en el TN para cada una de las cuatro existentes en la actualidad. La Operación Permanente en el Ciberespacio tendría su propio pasador con la inscripción *CIBERESPACIO*. Esta medalla se concedería por una involucración en la operación por un periodo continuado de dos años, que podrían ser acumulables, y sería valorada al mismo nivel que el resto de condecoraciones por participar en misiones en ZO. Además, esta medalla, que requiere o valora la permanencia del personal en el destino, resultará beneficiosa para el personal del MCCE comparativamente con el personal participante en las otras tres operaciones.

d) Sueldo: realizada la comparativa de los ingresos percibidos por un miembro del MCCE con respecto a otra unidad del Órgano Central (como la UME) o con respecto a expertos en ciberseguridad del entorno empresarial, se concluye que resulta necesario equiparar el sueldo del MCCE al menos al de la UME si se pretende conseguir un grado similar de captación.

   Además, dado que resulta prácticamente imposible equiparar los sueldos del personal del MCCE a los percibidos por profesionales con una formación similar y que realizan funciones parecidas en organizaciones civiles, la retención de estos profesionales será complicada si no se consigue que obtengan una proyección profesional dentro de la carrera militar. Esto se puede conseguir, como se ha reiterado a lo largo de este TFM, con la creación a corto-medio plazo del C.C. del Ciberespacio.

e) Proyección internacional: los miembros de las FAS valoran poder salir destinados o en comisión de servicio a vacantes en organismos internacionales. Lo cual se considera gratificante por motivos profesionales, familiares y económicos.

   Se propone que el CMCCE prele todas las vacantes y comisiones en el extranjero, tanto relacionadas con CIS como con Ciberdefensa. La cobertura de estas vacantes por personal destinado en el MCCE se puede considerar como *"win to win"* para el militar y para la institución.

   Además, se propone que a las vacantes internacionales relacionadas con el ciberespacio y a las plazas relacionadas con el personal CIS de la JSITFAS (en la actualidad JCISFAS) se le pueda exigir que cumplan condiciones de una serie de especialidades o cursos, y lo mismo para el personal de Ciberdefensa perteneciente actualmente a la FOCE y en un futuro al MOCE.

f) Formación: en la actualidad, el grado de formación del personal del MCCE se considera elevado, apoyándose en centros de referencia nacionales e internacionales. Por tal motivo, no se plantea ninguna propuesta de mejora, al considerar que la línea formativa que está siguiendo el MCCD en los últimos años es la adecuada para conseguir su fin.

Una vez abordado un diagnóstico relativo a las necesidades del personal para poder desarrollar su labor dentro del ámbito del ciberespacio y las acciones que se podrían acometer para conseguirlo, tanto en la situación actual en un reciente MCCE como a corto-medio plazo con la creación del Cuerpos Común del Ciberespacio o medio-largo plazo con un ejército independiente, hay que plantearse que no todo el personal podrá llegar a la cima piramidal de la organización. Esta es la razón por la que cobra importancia la reinserción laboral del personal operativo del ciberespacio, cuestión por la cual tiene que preocuparse el MCCE, pues no existe mejor publicidad para una empresa o institución que la que divulguen sus miembros cuando cesan en ella: trato recibido, fomento de su formación y consideración tanto personal como de sus aportaciones y propuestas.

En este contexto, aparece de nuevo el concepto "*Employer Branding*", el cual se puede definir, tal y como hemos abordado en el presente TFM, como un conjunto de medidas adoptadas por una organización encaminadas a conseguir que ésta resulte atractiva para los profesionales con talento. Por tanto, es un instrumento de gran utilidad para la captación y retención de personal, pero, en este caso, también para la reinserción laboral. Así, si el MCCE se convirtiese en un referente dentro del sector de la ciberseguridad, la ciberdefensa y la ciberinteligencia, y por ende su personal, junto con el la cualificación profesional de sus miembros, consideramos que se conseguirá que el perfil de un componente del MCCE sería valorado en gran medida por las empresas del sector.

Figura 2. Reinserción laboral del personal del ciberespacio (tomada [3])

Por tanto, se propone que el concepto "*Employer Branding*" no se enfoque en exclusividad a la captación de personal, sino también para la reinserción laboral de sus miembros. Si el MCCE consigue posicionarse como un referente en el sector de la ciberseguridad, la ciberdefensa y la ciberinteligencia, la lucha por la captación del talento en este sector tendrá un importante nicho de búsqueda en el Ejército del Ciberespacio.

3. Conclusiones

La finalidad del presente trabajo ha residido en plantear el posible futuro de las Fuerzas de Ciberdefensa en las FAS y, por consiguiente, definir un perfil de carrera específico para su personal. Para ello, se han reflejado una amplia gama de propuestas con el fin de alcanzar tal objetivo y así situar al ciberespacio como una prioridad dentro de las FAS; creando o potenciando, por tanto, el perfil

de carrera de su personal para poder llegar a tal fin. Así, a lo largo del TFM se han expuesto, partiendo de la situación actual de las Fuerzas de Ciberdefensa en las FAS y del perfil de carrera de su personal, posibles líneas de mejora con la finalidad de consolidar el ciberespacio como un ámbito de las operaciones al mismo nivel que el resto de los dominios.

Por otra parte, se abordan factores justificativos que demuestran la necesidad de crear un perfil específico *ciber* dentro de los Ejércitos y Armada, con la finalidad de conseguir que el personal que así lo desee pueda tener una trayectoria profesional sin penalización. Esto será un primer paso mientras no se consiga el objetivo prioritario que es la creación de un nuevo *Ejército del Ciberespacio* dentro de las FAS, que incluya tanto al personal CIS como de Ciberdefensa.

A modo de conclusión, se aportan, de forma razonada, una serie de argumentos que inducen la necesidad de conseguir un *Ejército del Ciberespacio* independiente de los Ejércitos y Armada, pues es la única manera de conseguir la especialización en este ámbito y que las operaciones en el ciberespacio sean lideradas por personal experto y con un nuevo estilo de dirección. La creación de este ejército permitiría entre otros aspectos:

- la consecución de un perfil de carrera apropiado para su personal y la permanencia del mismo,

- obtener una unidad con imagen de marca de empleador o *"Employer Branding"*, que originaría en el personal militar y civil un interés creciente por trabajar o colaborar en dicha unidad y, por último,

- conseguir que el perfil del profesional que haya formado parte de Ejército del Ciberespacio sea reconocido por el nivel de excelencia que posee en este ámbito (tanto por parte de las empresa civiles en los sectores de la ciberseguridad, la ciberdefensa y la ciberinteligencia, como en el contexto académico), con la finalidad de conseguir su reinserción laboral, en caso de que valorase finalizar su relación profesional con las FAS.

Referencias

1. PDC-01 (A) Doctrina para el empleo de las FAS.
2. NATO Cyber Defence Taxonomy and Definitions, 2014.
3. Página web My Chesco: https://www.mychesco.com/a/news/national/va-launches-solid-start-to-ensure-veterans-are-contacted-during-initial-transition/