Estado
Mayor de
la Defensa

Ciberseguridad en España:
Perspectiva del Mando Conjunto de Ciberdefensa

ETSIIT, Granada
16 Enero 2015

GD. Carlos Gómez López de Medina
Comandante Jefe del MCCD

- Ciberespacio:
  - Redes y sistemas conectados a internet, incluyendo redes sociales, a los que se accede desde dispositivos estáticos y/o móviles (“laptops”,“smartphones” y “tablets”).
  - Redes y sistemas no conectados a internet.

- El ciberespacio es un nuevo ámbito, (Tierra, Mar, Aire, Espacio, Ciberespacio), en el que también se planean, dirigen y ejecutan operaciones militares.

- Las acciones ofensivas en el ciberespacio son, con frecuencia, eficaces y siempre eficientes y de bajo riesgo para el atacante.

- Cualquier acción de “guerra convencional” está acompañada de acciones en el ciberespacio.

- En estas circunstancias, hay que disponer de las capacidades necesarias para proteger los intereses propios en el ciberespacio y responder de manera oportuna, legítima y proporcionada ante un ciberataque.

- Como sucede con frecuencia en situaciones de emergencia, las Fuerzas Armadas deben poder auxiliar a otras instituciones y organizaciones, públicas o privadas, cuando los intereses nacionales están en riesgo. La causa de ese riesgo puede ser un ciberataque.

ÍNDICE

- Estrategia de Seguridad Nacional. (10%)
  - Riesgos y amenazas para la Seguridad Nacional.
  - Ámbitos prioritarios de actuación y Líneas de Acción Estratégicas.

- Estrategia de Ciberseguridad Nacional. (45%)
  - Objetivos de la ciberseguridad.
  - Líneas de Acción para lograr los Objetivos de la ciberseguridad.
  - La ciberseguridad en el Sistema de Seguridad Nacional.

La Ciberdefensa en España y el MCCD

- Mando Conjunto de Ciberdefensa (MCCD). (40%)
  - Orden Ministerial de creación.
  - Responsabilidades, funciones y organización.
  - Operatividad: Proceso de IOC a FOC.
  - Objetivos.
- Conclusiones. (5%)
- Preguntas.

Estrategia de Seguridad Nacional

- Aprobada en Consejo de Ministros de 31 mayo 2013.
- 68 pág. Formato pdf en www.lamoncloa.gob.es
- Estructura:
  - Resumen Ejecutivo.
  - Capítulo 1. Una visión integral de la Seguridad Nacional.
  - Capítulo 2. La seguridad de España en el mundo.
  - Capítulo 3. Los riesgos y amenazas para la Seguridad Nacional.
  - Capítulo 4. Líneas de acción estratégicas.
  - Capítulo 5. Un nuevo Sistema de Seguridad Nacional.

Estrategia de Seguridad Nacional

Capítulo 3. Los riesgos y amenazas para la Seguridad Nacional

- Conflictos armados.
- Terrorismo.
- Ciberamenazas.
- Crimen organizado.
- Inestabilidad económica y financiera.
- Vulnerabilidad energética.
- Proliferación de armas de destrucción masiva.
- Flujos migratorios irregulares.
- Espionaje.
- Emergencias y catástrofes.
- Vulnerabilidad del espacio marítimo.
- Vulnerabilidad de las infraestructuras críticas y servicios esenciales.

Estrategia de Seguridad Nacional

Capítulo 3. Los riesgos y amenazas para la Seguridad Nacional

- Conflictos armados.
- Terrorismo.
- Ciberamenazas.
- Crimen organizado.
- Inestabilidad económica y financiera.
- Vulnerabilidad energética.
- Proliferación de armas de destrucción masiva.
- Flujos migratorios irregulares.
- Espionaje.
- Emergencias y catástrofes.
- Vulnerabilidad del espacio marítimo.
- Vulnerabilidad de las infraestructuras críticas y servicios esenciales.

Estrategia de Seguridad Nacional

Capítulo 4. Ámbitos prioritarios de actuación.

- Defensa nacional.
- Lucha contra el terrorismo.
- Ciberseguridad.
- Lucha contra el crimen organizado.
- Seguridad económica y financiera.
- Seguridad energética.
- No proliferación de armas de destrucción masiva.
- Ordenación de flujos migratorios.
- Contrainteligencia.
- Protección ante emergencias y catástrofes.
- Seguridad marítima.
- Protección de las infraestructuras críticas.

ÍNDICE

Estrategia de Ciberseguridad Nacional

- Aprobada el Consejo de Seguridad Nacional el 05 de diciembre de 2013.
- 55 pág. Formato pdf en www.lamoncloa.gob.es
- Estructura:
  - Resumen Ejecutivo.
  - Capítulo 1. El ciberespacio y su seguridad.
  - Capítulo 2. Propósito y principios rectores de la ciberseguridad en España.
  - Capítulo 3. Objetivos de la ciberseguridad.
  - Capítulo 4. Líneas de acción de la ciberseguridad Nacional.
  - Capítulo 5. La ciberseguridad en el Sistema de Seguridad Nacional.

Estrategia de Ciberseguridad Nacional

Capítulo 3. Objetivos de la ciberseguridad

- Un Objetivo Global: Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques.

- Seis Objetivos Específicos.

ÍNDICE

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Línea de Acción 1. Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas.

- Contenido: Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Implicaciones expresas para el MINISDEF de la LA-1.
  - Ampliar y mejorar permanentemente las capacidades de Ciberdefensa de las FAS.
  - Se consolidará la implantación del Mando Conjunto de Ciberdefensa.
  - Potenciar las capacidades militares y de inteligencia para ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Línea de Acción 2. Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas.

- Contenido: Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.

- Implicaciones expresas para el MINISDEF.
  - Reforzar las estructuras de seguridad y la capacidad de vigilancia de los Sistemas de Información, en particular los que manejan información clasificada.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Línea de Acción 3. Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas.

- Contenido: Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.

- Implicaciones expresas para el MINISDEF.
  - Inicialmente ninguna.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Línea de Acción 4. Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia.

- Contenido: Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.

- Implicaciones expresas para el MINISDEF.
  - Ninguna.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Línea de Acción 5. Seguridad y resiliencia de las TIC en el sector privado.

- Contenido: Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios, empleando instrumentos de cooperación público-privada.

- Implicaciones expresas para el MINISDEF.
  - Ninguna.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Línea de Acción 6. Conocimientos, competencias e I+D+i.

- Contenido: Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Implicaciones para el MINISDEF (El Gobierno de España procederá a) de la LA-6. Especialmente:
  - Desarrollar un Marco de Conocimientos de Ciberseguridad en los ámbitos técnico, operativo y jurídico.
  - Extender y ampliar los programas de captación de talento, investigación avanzada y capacitación en ciberseguridad en cooperación con Universidades y centros especializados.
  - Establecer los mecanismos que permitan identificar de forma temprana las prioridades y demandas de los poderes públicos en materia de ciberseguridad para su incorporación a las iniciativas anteriores.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Línea de Acción 7. Cultura de ciberseguridad.

- Contenido: Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.

- Implicaciones para el MINISDEF.
  - Desarrollar la cultura de ciberseguridad en el Ministerio (140.000 / 90.000).

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Línea de Acción 8. Compromiso Internacional.

- Contenido: Promover un ciberespacio internacional seguro y confiable, en apoyo de los intereses nacionales.

Estrategia de Ciberseguridad Nacional

Capítulo 4. Líneas de acción.

- Implicaciones para el MINISDEF (El Gobierno de España desarrollará) de la LA-8 .
  - Potenciar la presencia de España en organizaciones y foros internacionales.
  - Propiciar la suscripción de acuerdos en el seno de organizaciones internacionales y con los principales socios y aliados.
  - Promover la participación coordinada de instituciones públicas y privadas en simulacros y ejercicios internacionales.
  - Fomentar la cooperación con la OTAN en materia de ciberdefensa.

ÍNDICE

Estrategia de Ciberseguridad Nacional

Capítulo 5. Sistema de Seguridad Nacional

- Consejo de Seguridad Nacional.
  - Presidencia y Vocales.
  - Ley Orgánica de Seguridad Nacional.
- Consejo Nacional de Ciberseguridad.
  - Vocales (13).
    - Presidencia del Gobierno. Departamento de Seguridad Nacional.
    - Mº Asuntos Exteriores y Cooperación.
    - Mº Justicia.
    - Mº Defensa.

- Mº Hacienda y Administraciones Públicas.
- Mº Interior.
- Mº Fomento.
- Mº Educación, Cultura y Deporte.
- Mº Empleo y Seguridad Social.
- Mº Economía y Competitividad.
- Mº Industria, Energía y Turismo.
- Mº Presidencia.
- Centro Nacional de Inteligencia (CNI).

Estrategia de Ciberseguridad Nacional

Capítulo 5. Sistema de Seguridad Nacional

- Presidencia del Consejo.
  - Rotativa y anual.
  - Centro Nacional de Inteligencia.
  - Mº Interior.
  - Mº Industria, energía y turismo.
  - Mº Defensa.
  - Mº Exteriores y cooperación.
- Apoyado por el Departamento de Seguridad Nacional.
- Plan Nacional de Ciberseguridad.

La Ciberdefensa en España y el MCCD

- Mando Conjunto de Ciberdefensa (MCCD). (40%)
  - Orden Ministerial de creación.
  - Responsabilidades, funciones y organización.
  - Operatividad: Proceso de IOC a FOC.
  - Objetivos.
- Conclusiones. (5%)
- Preguntas.

Ciberdefensa Militar EMAD
Capacidades

- Capacidad de Defensa. "… protección de los sistemas de información y comunicaciones, y la información que manejan, frente a ciberataques y su recuperación en caso de fallo o inutilización, parcial o total". Ciberseguridad.

- Capacidad de Explotación. "… obtención de información sobre las capacidades cibernéticas de defensa, explotación y respuesta de potenciales adversarios y agentes hostiles."

- Capacidad de Respuesta (Ataque). "… realización de ciberataques como defensa frente a amenazas y ataques".

Creación del MCCD

Orden Ministerial 10/2013

Ámbito de actuación del MCCD

- Redes y sistemas de información y telecomunicaciones de las FAS (>MDEF).
- Aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional.

Misión del MCCD

- Planeamiento y ejecución de las acciones relativas a la Ciberdefensa Militar.
- Contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

Creación del MCCD

Orden Ministerial 10/2013

Cometidos del MCCD (1/3)

1. Garantizar el libre acceso al ciberespacio, con el fin de cumplir las misiones y cometidos asignados a las Fuerzas Armadas, mediante el desarrollo y empleo de los medios y procedimientos necesarios.

2. Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la manejan y tenga encomendados.

3. Garantizar el funcionamiento de los servicios críticos de los sistemas de las FAS en un ambiente degradado debido a incidentes, accidentes o ataques.

Creación del MCCD

Orden Ministerial 10/2013

Cometidos del MCCD (2/3)

4. Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas de su responsabilidad.

5. Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

6. Dirigir y coordinar, en materia de ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y Armada y el de operaciones de seguridad de la información del Ministerio de Defensa.

Creación del MCCD

Orden Ministerial 10/2013

Cometidos del MCCD (3/3)

7. Ejercer la representación del Ministerio de Defensa en materia de ciberdefensa militar en el ámbito nacional e internacional.

8. Cooperar, en materia de ciberdefensa, con los centros nacionales de respuesta a incidentes de seguridad de la información, de acuerdo con lo que determinen las estrategias y políticas nacionales de ciberseguridad en vigor, así como con otros centros militares de respuesta a incidentes de seguridad de la información en el ámbito internacional.

9. Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa.

Creación del MCCD

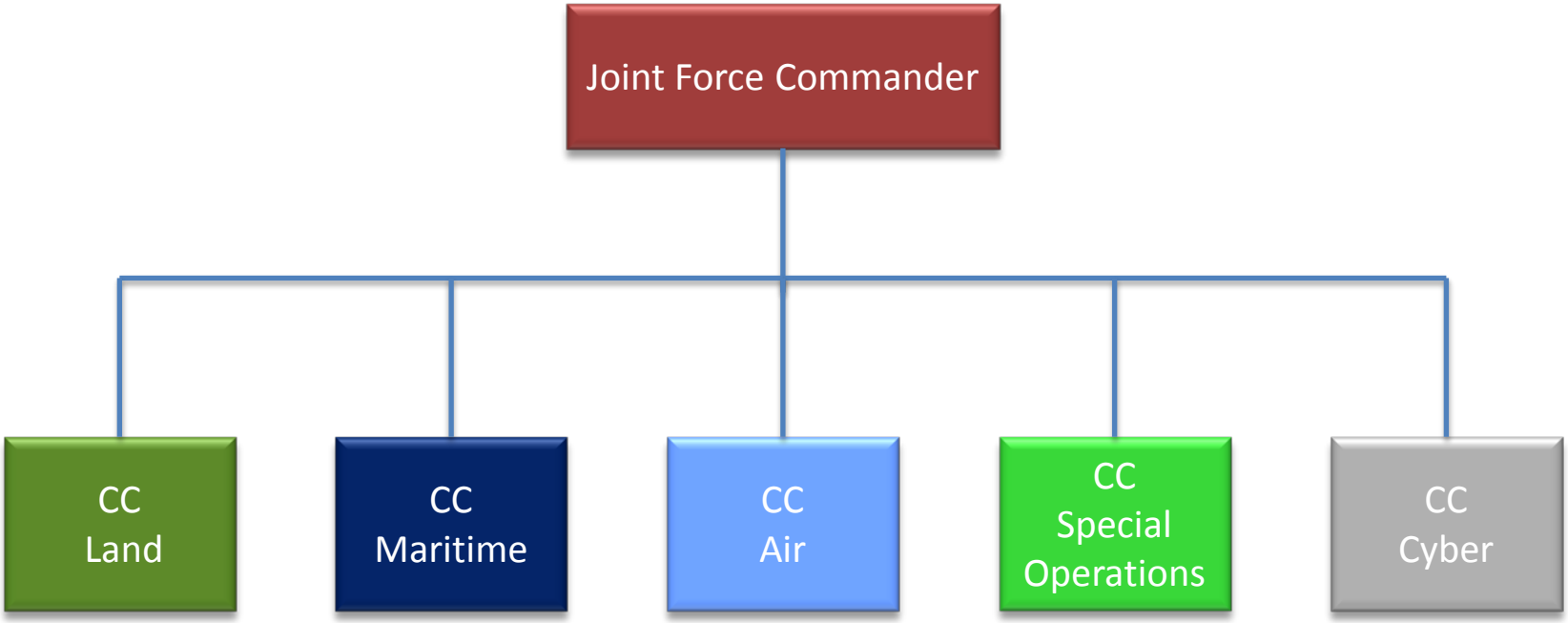
Orden Ministerial 10/2013

Mando y Dependencias

- El Comandante Jefe del MCCD dependerá orgánicamente del Jefe de Estado Mayor de la Defensa.

- El MCCD será un órgano perteneciente al Estado Mayor de la Defensa, integrado en la estructura operativa de las Fuerzas Armadas.

Estructura Fuerza Conjunta



La Ciberdefensa en España y el MCCD

- Mando Conjunto de Ciberdefensa (MCCD). (40%)
  - Orden Ministerial de creación.
  - Responsabilidades, funciones y organización.
  - Operatividad: Proceso de IOC a FOC.
  - Objetivos.
- Conclusiones. (5%)
- Preguntas.

Responsabilidades en España

- Mº Interior.
  - Infraestructuras Críticas.
  - Ciberdelito.
  - Ciberterrorismo.
- Centro Criptológico Nacional.
  - Administraciones Públicas.
- Mº Industria.
  - Asesorar a empresas públicas y privadas.
- Mº Defensa.
  - Sistemas información y telecomunicaciones del MDEF.
  - Sistemas de interés Defensa Nacional que se le asignen.
  - Acciones ofensivas.

Responsabilidades en MINISDEF (1/3)

- Capacidad de Defensa:
  - Ejércitos, Armada y MCCD son responsables de las redes y sistemas que tienen asignados, de acuerdo con las directrices del JEMAD.
  - MCCD dirige y coordina a los centros de operaciones de seguridad del Ministerio.
  - MCCD coopera con centros nacionales e internacionales de respuesta en representación del Ministerio.
- Capacidad de Explotación: MCCD.
- Capacidad de Ataque: MCCD.

Responsabilidades en MINISDEF (2/3)

- Concienciación, formación y adiestramiento: El MCCD es responsable de la definición, dirección y coordinación.

- Representación nacional e internacional del Ministerio: MCCD.

Responsabilidades en MINISDEF (3/3)

- Es voluntad del MCCD, y condición necesaria para el éxito, impulsar la suma de esfuerzos y recursos existentes en el Ministerio de Defensa.
- El MCCD impulsará con intensidad la coordinación a todos los niveles:
  - Mº Defensa: Ejércitos, Armada e ITM.
  - Administración: CNI, Ministerios (Interior, Industria, etc.) y otras administraciones públicas.
  - Empresas especializadas y Universidades.
  - Organismos Internacionales.
  - Fuerzas Armadas aliadas (UE, OTAN, Iberoamérica, etc.).

Estado Mayor de la Defensa

Funciones

0. Mando

Estado Mayor

1. Planeamiento
2. Doctrina
3. Cooperación
4. Representación
5. Formación
6. Gestión del Conocimiento

Operaciones

7. Monitorización
8. Gestión de Incidentes
9. Inspección y Acreditación
10. Apoyo Técnico
11. Análisis de actividad

Operaciones

12. Explotación de la Información
13. Ejecución de Operaciones
14. Campo de Maniobras
15. Actualización Tecnológica
16. Desarrollo de Productos
17. Desarrollo de Ciberarmas

JAS

18. Gestión Administrativa
19. Obtención de Recursos
20. Seguridad de la Información
21. Administración CIS
22. Asesoramiento Legal

Estado Mayor de la Defensa

Organización

La Ciberdefensa en España

- Mando Conjunto de Ciberdefensa (MCCD). (40%)
  - Orden Ministerial de creación.
  - Responsabilidades, funciones y organización.
  - Operatividad: Proceso de IOC a FOC.
  - Objetivos.
- Conclusiones. (5%)
- Preguntas.

Operatividad: IOC ➡ FOC

La Ciberdefensa en España

- Mando Conjunto de Ciberdefensa (MCCD). (40%)
  - Orden Ministerial de creación.
  - Responsabilidades, funciones y organización.
  - Operatividad: Proceso de IOC a FOC.
  - Objetivos.
- Conclusiones. (5%)
- Preguntas.

Objetivos del MCCD

A Corto/Medio Plazo (1/2)

- Operar en coordinación con el Mando de Operaciones (MOPS) y el Centro de Inteligencia de las Fuerzas Armadas (CIFAS).
- Poner en práctica el Plan y Programas de concienciación, formación y adiestramiento para todo el Mº de Defensa.
- Llevar a cabo la dirección y coordinación de las capacidades defensivas de los Ejércitos, Armada y Órgano Central del Ministerio de Defensa.
- Adecuar los recursos de personal a las necesidades operativas.
- Alcanzar la Capacidad Operativa Final en Defensa, Explotación y Respuesta.

Objetivos del MCCD

A Corto/Medio Plazo (2/2)

- Obtener la aprobación del presupuesto necesario para cada anualidad.

- Colaborar en la consecución de los objetivos que se establecen en Estrategia de Ciberseguridad Nacional.
  - Coordinar estrechamente con organismos de la Administración Pública.
  - Impulsar el desarrollo industrial y reforzar el sistema de I+D+i.
  - Aumentar la cultura de ciberseguridad.
  - Promover y sostener el compromiso internacional con organizaciones internacionales y con las Naciones aliadas.

Objetivos del MCCD

A Largo Plazo

(Objetivos permanentes)

- Desarrollar las Capacidades de Defensa, Explotación y Respuesta.
- Evolucionar el Plan y los Programas de concienciación, formación y adiestramiento.
- Colaborar en la consecución de los objetivos establecidos en la Estrategia de Ciberseguridad Nacional en vigor.

La Ciberdefensa en España

- Mando Conjunto de Ciberdefensa (MCCD). (40%)
  - Orden Ministerial de creación.
  - Responsabilidades, funciones y organización.
  - Operatividad: Proceso de IOC a FOC.
  - Objetivos.
- Conclusiones. (5%)
- Preguntas.

CONCLUSIONES

- La ECSN contempla 7 Objetivos y 8 Líneas de Acción para lograrlos.

- La ECSN recoge la importancia de las Fuerzas Armadas y, en concreto, del MCCD para alcanzar los Objetivos marcados.

- La ECSN incluye la acción ofensiva cuando se cumplen las condiciones de oportunidad, legalidad y proporcionalidad.

CONCLUSIONES

- El Consejo Nacional de Ciberseguridad es el órgano encargado de dirigir, coordinar y velar por la correcta implantación de la ECSN.

- Los cometidos y objetivos del Mando Conjunto de Ciberdefensa son coherentes con las Líneas de Acción de la ECSN.

La Ciberdefensa en España

- Mando Conjunto de Ciberdefensa (MCCD). (40%)
  - Orden Ministerial de creación.
  - Responsabilidades, funciones y organización.
  - Operatividad: Proceso de IOC a FOC.
  - Objetivos.
- Conclusiones. (5%)
- Preguntas.

Estado
Mayor de
la Defensa

Ciberseguridad en España:
Perspectiva del Mando Conjunto de Ciberdefensa

ETSIIT, Granada
16 Enero 2015

GD. Carlos Gómez López de Medina
Comandante Jefe del MCCD