La Ciberdefensa en el contexto de la nueva Estrategia de Seguridad Nacional

Semana Naval de la Armada

Jornadas Tecnológicas
24 septiembre 2013

GB. Carlos Gómez López de Medina
Comandante Jefe del
Mando Conjunto de Ciberdefensa

- La amenaza existe, aunque el sistema no esté conectado a internet.

- La amenaza existe, aunque el sistema no esté conectado a internet.
- 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.

- La amenaza existe, aunque el sistema no esté conectado a internet.
- 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.

- La amenaza existe, aunque el sistema no esté conectado a internet.
- 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.

- La amenaza existe, aunque el sistema no esté conectado a internet.
- 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” estará 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.

- 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.
  - Riesgos y amenazas para la Seguridad Nacional.
  - Ámbitos prioritarios de actuación y Líneas de Acción Estratégicas.
  - Ciberseguridad.
- Mando Conjunto de Ciberdefensa (MCCD).
  - Orden Ministerial de creación.
  - Responsabilidades.
  - Operatividad: IOC ➡ FOC.
  - Objetivos.
- Conclusiones.

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. "… realización de ciberataques como defensa frente a amenazas y ataques".

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 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.

Estrategia de Seguridad Nacional

Capítulo 4. Ciberseguridad.
Líneas de Acción Estratégicas.

Objetivo. Garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques.

1. Incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas con apoyo en un marco jurídico operativo y eficaz.

2. Garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas.

Estrategia de Seguridad Nacional

Capítulo 4. Líneas de acción estratégicas. Ciberseguridad.

3. Colaboración público-privada. Se impulsarán y liderarán actuaciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial.

4. I+D+i. Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española a través de un Plan de I+D+i.

Estrategia de Seguridad Nacional

Capítulo 4. Líneas de acción estratégicas. Ciberseguridad.

5. Concienciación. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.

6. Colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional donde se alineen las iniciativas de todos los países que persiguen un entorno seguro y fiable.

ÍNDICE

Creación del MCCD

Orden Ministerial 10/2013

Ámbito de actuación del MCCD

- Redes y sistemas de información y telecomunicaciones de las FAS.
- 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

MINISTERIO DE DEFENSA

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 será un Oficial General de los Cuerpos Generales del Ejército de Tierra, de la Armada, del Ejército del Aire, o del Cuerpo de Infantería de Marina, dependiente 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.

ÍNDICE

- Estrategia de Seguridad Nacional.
  - Riesgos y amenazas para la Seguridad Nacional.
  - Ámbitos prioritarios de actuación y Líneas de Acción Estratégicas.
  - Ciberseguridad.
- Mando Conjunto de Ciberdefensa (MCCD).
  - Orden Ministerial de creación.
  - Responsabilidades.
  - Operatividad: IOC ➡ FOC.
  - Objetivos.
- Conclusiones.

Responsabilidades en MINISDEF (1/3)

- Defensa:
  - Ejércitos, Armada, SDGTIC 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 respuesta del Ministerio.
  - MCCD coopera con centros nacionales e internacionales de respuesta en representación del Ministerio.
- Explotación: MCCD.
- Respuesta: MCCD.

Responsabilidades en MINISDEF (2/3)

- Concienciación, formación y adiestramiento: El MCCD es responsable de la definición, dirección y coordinación. Ejércitos, Armada, SDGTIC y MCCD son responsables de la formación, preparación y adiestramiento de su personal.

- 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, SDGTIC 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.).

ÍNDICE

- Estrategia de Seguridad Nacional.
  - Riesgos y amenazas para la Seguridad Nacional.
  - Ámbitos prioritarios de actuación y Líneas de Acción Estratégicas.
  - Ciberseguridad.
- Mando Conjunto de Ciberdefensa (MCCD).
  - Orden Ministerial de creación.
  - Responsabilidades.
  - Operatividad: IOC ➡ FOC.
  - Objetivos.
- Conclusiones.

Operatividad: IOC ➡ FOC

ÍNDICE

- Estrategia de Seguridad Nacional.
  - Riesgos y amenazas para la Seguridad Nacional.
  - Ámbitos prioritarios de actuación y Líneas de Acción Estratégicas.
  - Ciberseguridad.
- Mando Conjunto de Ciberdefensa (MCCD).
  - Orden Ministerial de creación.
  - Responsabilidades.
  - Operatividad: IOC ➡ FOC.
  - Objetivos.
- Conclusiones.

Objetivos del MCCD

- En 2013.
- A Corto Plazo.
- A Medio y Largo Plazo.

Objetivos del MCCD
En 2013

- Alcanzar la Capacidad Operativa Inicial el 27sep13.
- Comenzar a operar en coordinación con el Mando de Operaciones (MOPS) y el Centro de Inteligencia de las Fuerzas Armadas (CIFAS).
- Dar a conocer el MCCD.
- Obtener la aprobación del presupuesto para 2014.
- Firma de la ampliación del Convenio de Colaboración existente entre la UPM y el Mº de Defensa para incorporar la Ciberdefensa.

Objetivos del MCCD
A Corto Plazo

- Diseñar los planes de formación y concienciación.
- Llevar a cabo la dirección y coordinación de las capacidades defensivas de los Ejércitos, Armada y Mº de Defensa.
- Completar la plantilla de personal militar.
- Iniciar la coordinación con organismos ajenos al Mº de Defensa (Nacionales e Internacionales).
- Alcanzar la Capacidad Operativa Final en Defensa, Explotación y Respuesta.

Objetivos del MCCD
A Medio y Largo Plazo

- Impulsar la concienciación, formación y adiestramiento sobre Ciberdefensa.
- Desarrollar las Capacidades de Defensa, Explotación y Respuesta.
- Fomentar la coordinación con organismos ajenos al Mº de Defensa.
- Fomentar las actividades de I+D+i y la colaboración con empresas y universidades.

ÍNDICE

CONCLUSIONES

- La Estrategia Nacional de Seguridad establece "Los 12 riesgos y amenazas para la Seguridad Nacional". Entre ellos se encuentran las Ciberamenazas.

- También determina los 12 ámbitos prioritarios de actuación. Cada uno de ellos contempla unas "Líneas de Acción Estratégicas" para hacer frente a los riesgos y amenazas.

- La Ciberseguridad es uno de los ámbitos prioritarios de actuación e incluye 6 Líneas de Acción Estratégicas.

- Los cometidos y objetivos del Mando Conjunto de Ciberdefensa son coherentes con las Líneas de Acción Estratégicas de la Ciberseguridad y de otros ámbitos prioritarios de actuación.

La Ciberdefensa en el contexto de la nueva Estrategia de Seguridad Nacional

Semana Naval de la Armada

Jornadas Tecnológicas
24 septiembre 2013

GB. Carlos Gómez López de Medina
Comandante Jefe del
Mando Conjunto de Ciberdefensa