

**XIII
JORNADAS
STIC
CCN-CERT**



Operaciones en el ciberspacio



**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



C.C. Carlos A. Santos Sande

Analista de Operaciones EM del Mando Conjunto de Ciberdefensa

MCCD / Ministerio de Defensa

Índice

- 1. Ciberespacio, nuevo campo de batalla**
- 2. Operaciones en el ciberespacio**
- 3. Capacidades operativas**
- 4. MCCD en la estructura conjunta de las FAS**
- 5. Conducción de operaciones**



Ciberspacio, nuevo campo de batalla

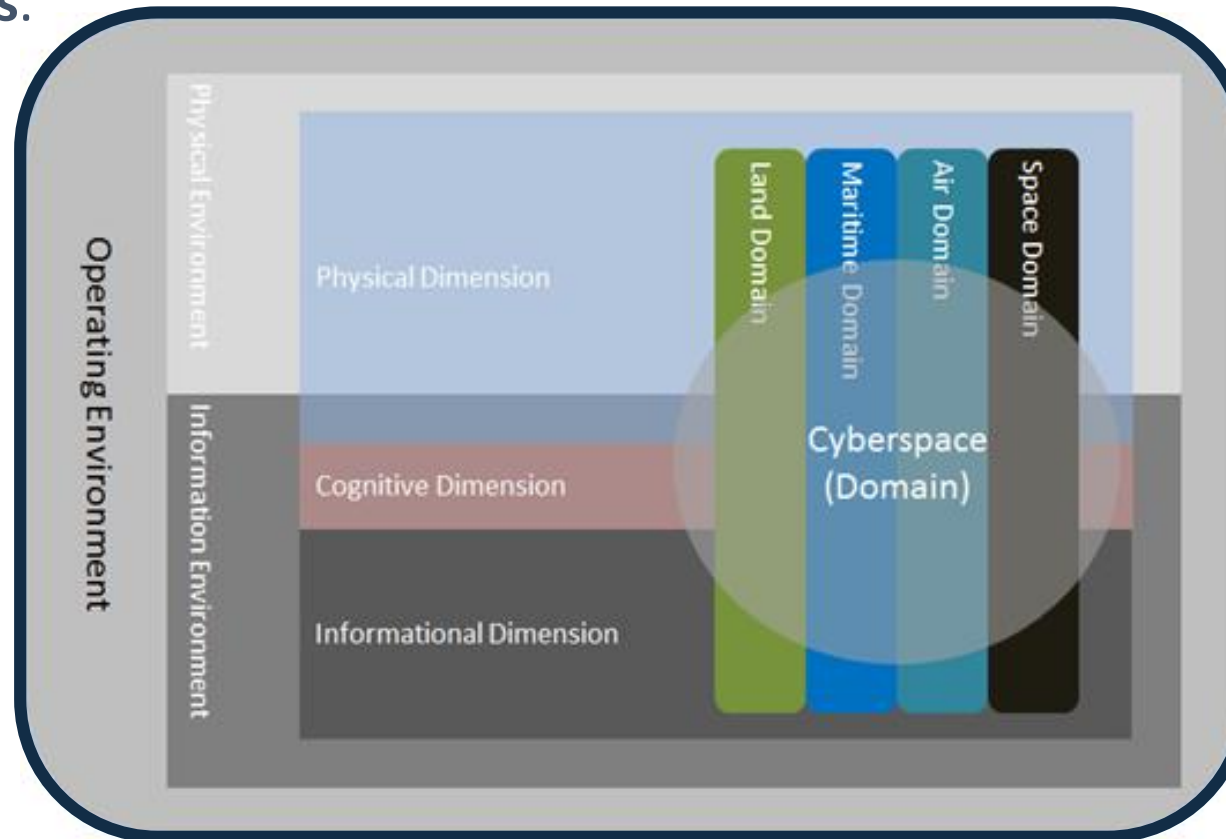


Ciberespacio, nuevo campo de batalla



Ciberspacio, nuevo campo de batalla

Cumbre OTAN de Varsovia JUL16, se reconoce el ciberespacio como el quinto dominio de las operaciones militares.



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**.

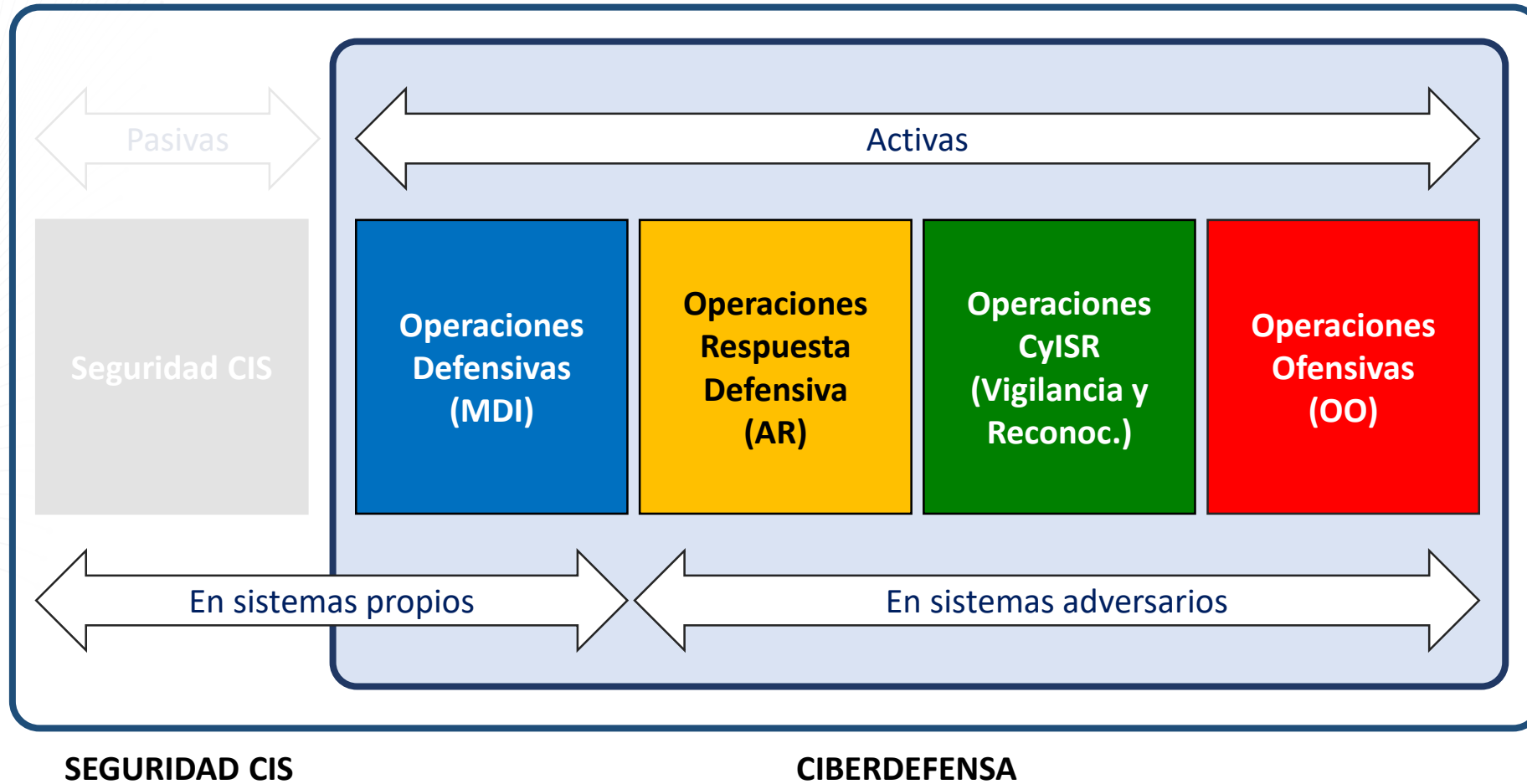
(NATO Cyber Defence Taxonomy and Definitions, 2014)



Operaciones en el ciberespacio



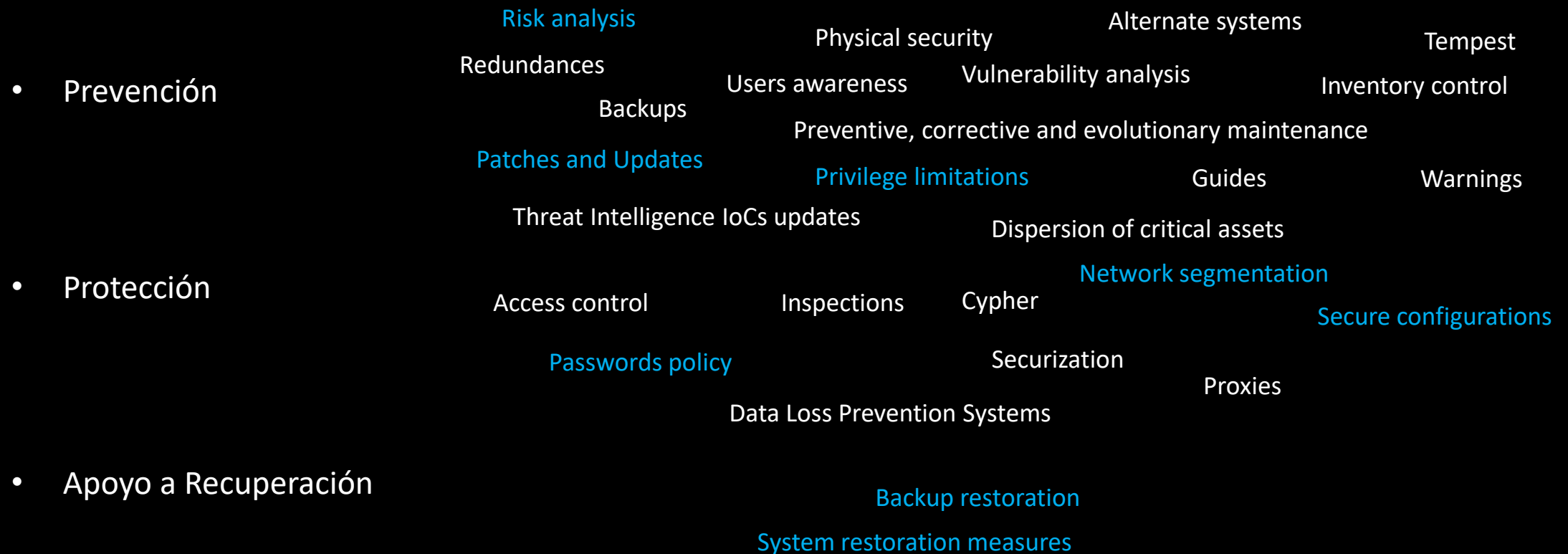
Operaciones en el ciberespacio



Operaciones en el ciberespacio

Ciberseguridad/Seguridad CIS

Seguridad CIS/Ciberseguridad: Conjunto de medidas y acciones enfocadas a que las redes y sistemas operen con seguridad (**preventivas**, de **protección** y de apoyo a la **recuperación**).



Operaciones en el ciberespacio

Operaciones Defensivas

Conjunto de medidas y acciones encaminadas a **detectar, identificar, interceptar, rechazar y neutralizar** todo tipo de ataques o intentos de penetración en el **AOCD**.

Operaciones Defensivas (MDI)

Medidas y acciones dentro de la infraestructura propia encaminadas a detectar, identificar, interceptar, rechazar y neutralizar todo tipo de ataques o intentos de penetración en el AOCD.



Operaciones de Respuesta Defensiva (AR)

Medidas y acciones en la infraestructura del adversario encaminadas a neutralizar todo tipo de ataques o intentos de penetración en el AOCD.

Operaciones en el ciberespacio

Operaciones Defensivas

Medidas y acciones

MDI

- Monitorización.
- Correlación de eventos.
- Gestión de incidentes.
- Detección.
- Detención.
- Diversión.
- Decepción.
- Dilación.
- Degradación.
- Generación de IoC.
- Solución nuevas vulnerabilidades.
- Etc...

AR

- Infiltración.
- Captura.
- Perturbación.
- Denegación de uso.
- Degradación.
- Alteración.
- Interrupción.
- Etc...



Operaciones en el ciberespacio

Operaciones de Vigilancia y Reconocimiento

Conjunto de acciones orientadas a la **obtención, análisis y aprovechamiento de información** sobre las **capacidades ciber del adversario**.

Proporcionar a los equipos de operaciones defensivas

la información necesaria sobre las amenazas en el ciberespacio y en la AOCD, para la generación de Indicadores de Compromiso (IoC), tácticas, técnicas y procedimientos de Defensa.



Proporcionar a los equipos de operaciones ofensivas

la información necesaria sobre las capacidades defensivas del adversario, vulnerabilidades, sistemas operativos, infraestructuras, identidades, etc.

Proporcionar al Comandante de la Ciberdefensa

el conocimiento de la situación externa sobre las capacidades, estado, intenciones, acciones y situación de los medios de ciberdefensa del adversario (CySA).

Operaciones en el ciberespacio

Operaciones de Vigilancia y Reconocimiento

Medidas y acciones

- Levantamiento del ORBAT Ciber adversario.
- Análisis de la amenaza:
 - Intenciones.
 - Capacidades.
 - Tácticas, técnicas y procedimientos.
- Extracción de información:
 - OSINT.
 - Otras fuentes.
- Colocación de señuelos.
- Análisis de vulnerabilidades.
- Ingeniería social.
- Test de penetración.

Operaciones en el ciberespacio

Operaciones Ofensivas

Acciones contra potenciales **adversarios** y agentes hostiles que afectan a la **integridad y disponibilidad** de sus **sistemas de información y telecomunicaciones** y/o a la información que manejan.

Acciones de fuerza militar en el ciberespacio de carácter estratégico, operacional o táctico:

- Acciones aisladas específicas.
- Como Mando Componente.
- Apoyo de las operaciones de otros Mandos Componentes.



Respuesta oportuna, legítima y proporcionada a las amenazas o agresiones en el ciberespacio que puedan afectar a la Defensa Nacional.

Vectores para la realización de **operaciones de Influencia.**

Operaciones en el ciberespacio

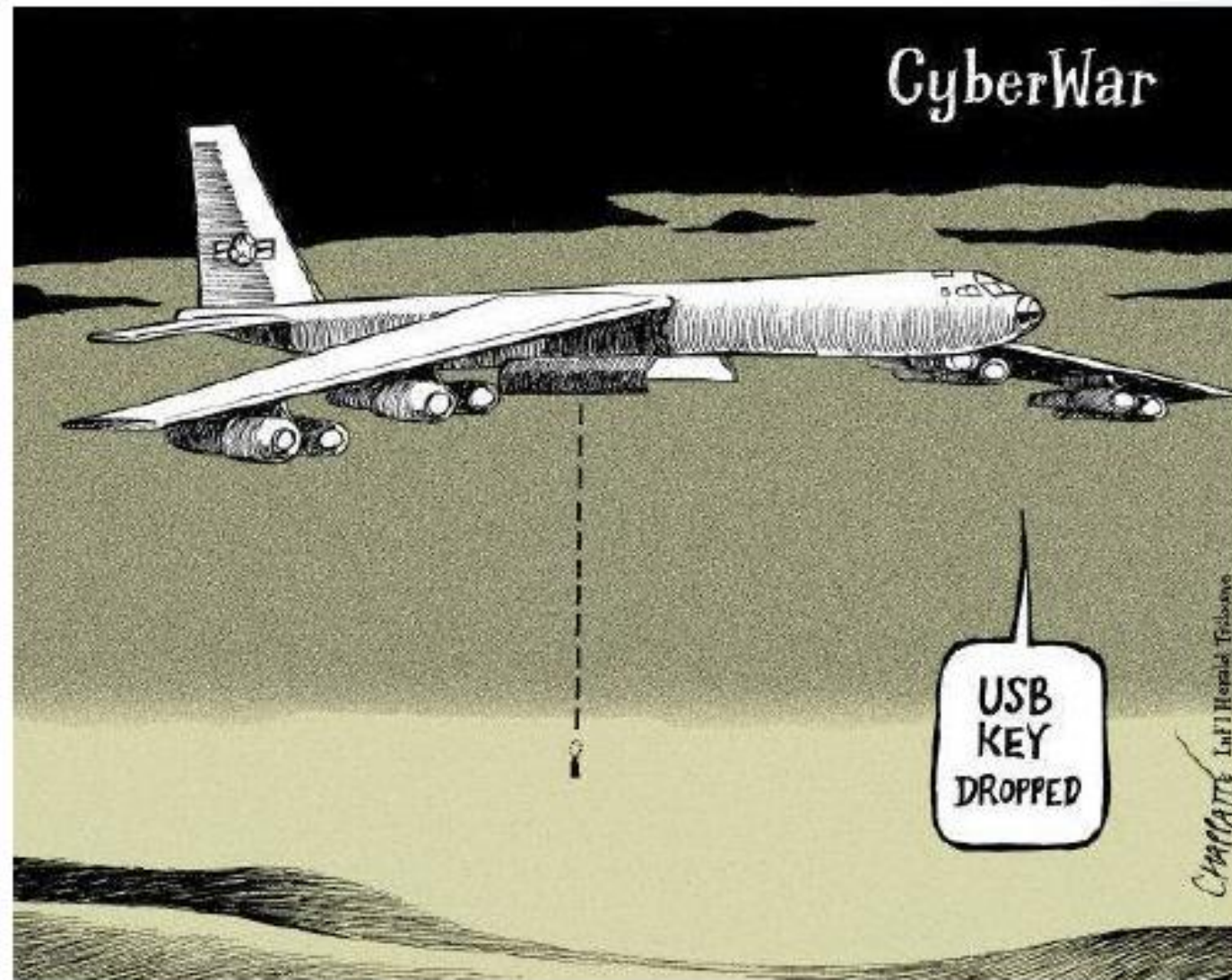
Operaciones Ofensivas

Medidas y acciones

- Infiltración.
- Captura.
- Perturbación.
- Denegación de uso.
- Degradación.
- Alteración.
- Interrupción.
- Etc...



Operaciones en el ciberespacio



Capacidades operativas



Capacidades operativas

DEFENSA

PREVENTIVA
PROACTIVA
REACTIVA



EXPLOTACIÓN

ALERTA TEMPRANA
CONOCIMIENTO SITUACION
INTELIGENCIA



RESPUESTA

OPORTUNA
LEGÍTIMA
PROPORCIONADA



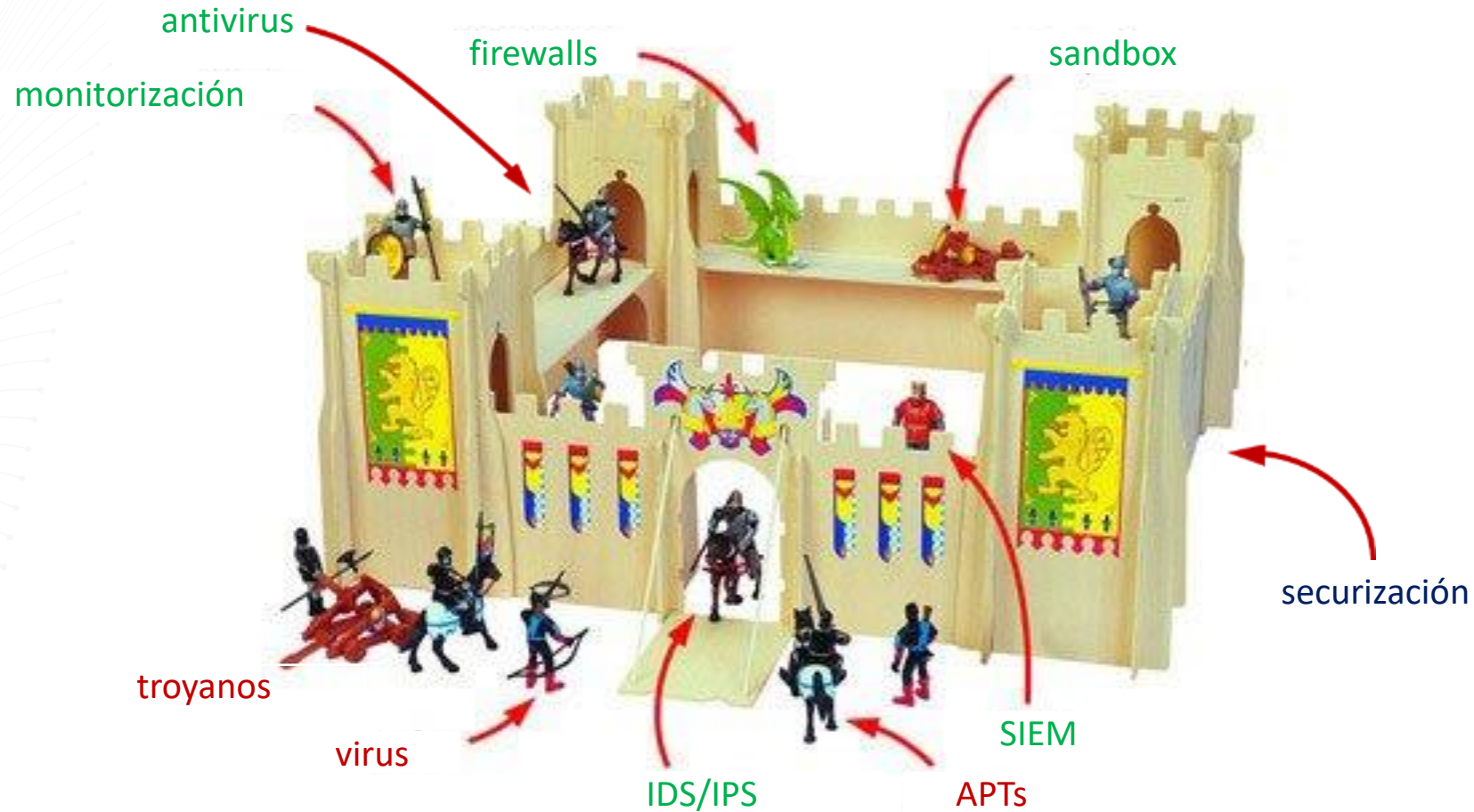
Capacidades operativas

Seguridad CIS/Ciberdefensa



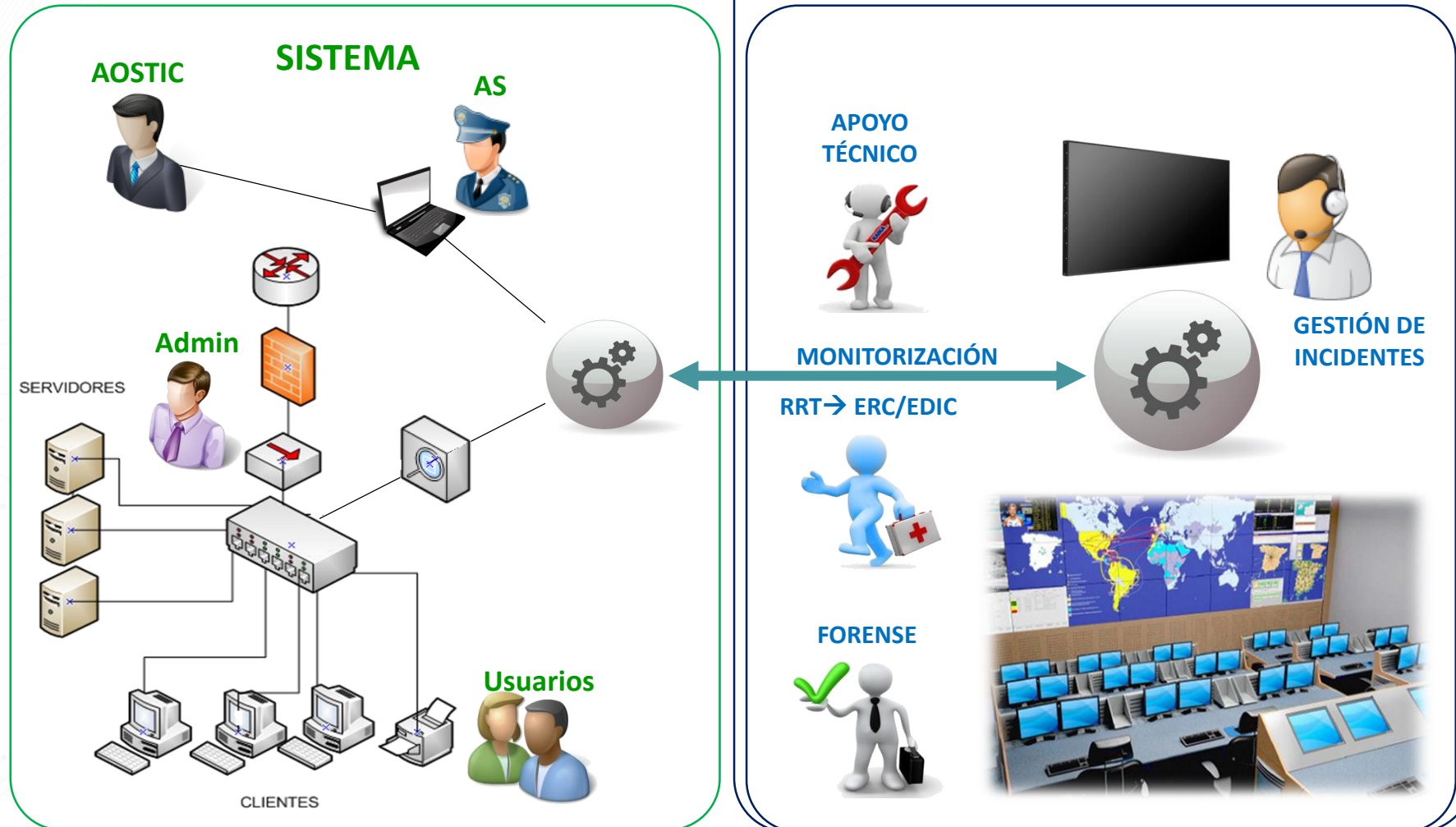
Capacidades operativas

Ciberdefensa vs Seguridad CIS



Capacidades operativas

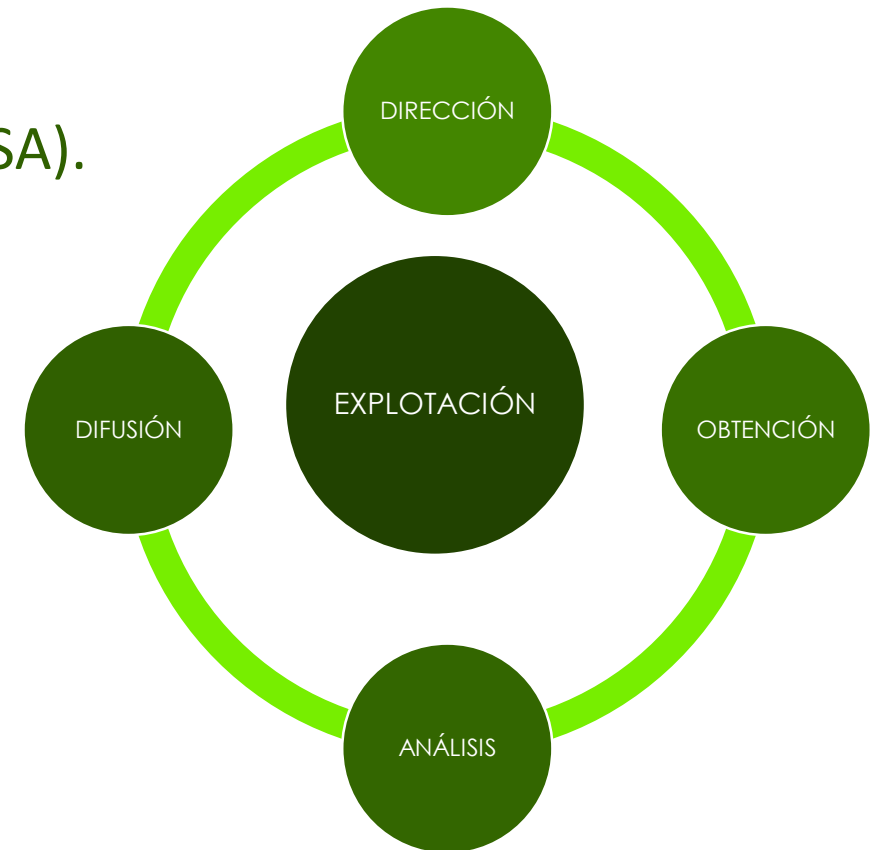
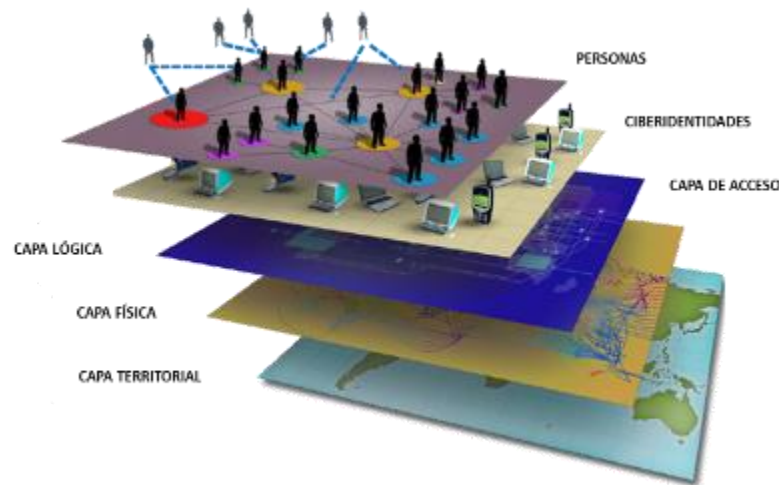
Capacidad de Defensa → ESP-DEF-CERT



Capacidades operativas

Capacidad de Explotación

- Inteligencia de ciberamenazas.
- Alerta temprana - Cyber Situational Awareness (CySA).
- Apoyo al Planeamiento de Operaciones.
- Contextualización incidentes (¿quién? ¿por qué?).



Capacidades operativas

Capacidad de Respuesta/Ataque

En caso de conflicto, las acciones ofensivas en el ciberespacio pueden ser un opción (y, a veces, la mejor opción).

Condiciones:

- Oportunidad.
- Legitimidad.
- Proporcionalidad.

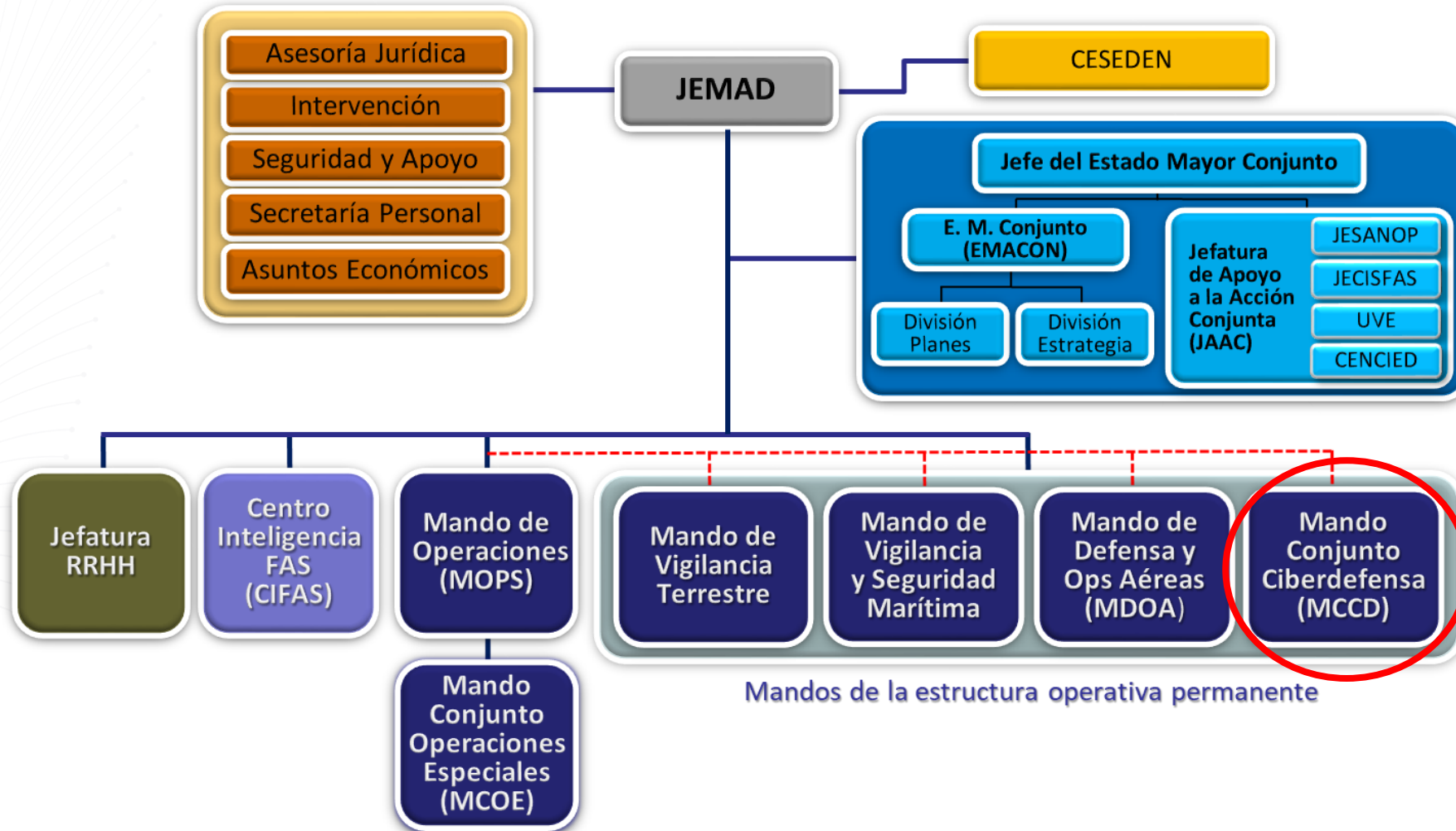
¿Qué se necesita?

- Ciberarmas (exploits, payloads, zero-days, etc....).
- Hackers.
- Ingenieros sociales.
- Entornos seguros para pruebas y entrenamiento.
- Infraestructura y herramientas para suplantación/anonimización.



MCCD en la estructura conjunta de las FAS

MCCD en la estructura conjunta de las FAS

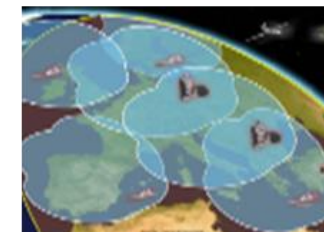
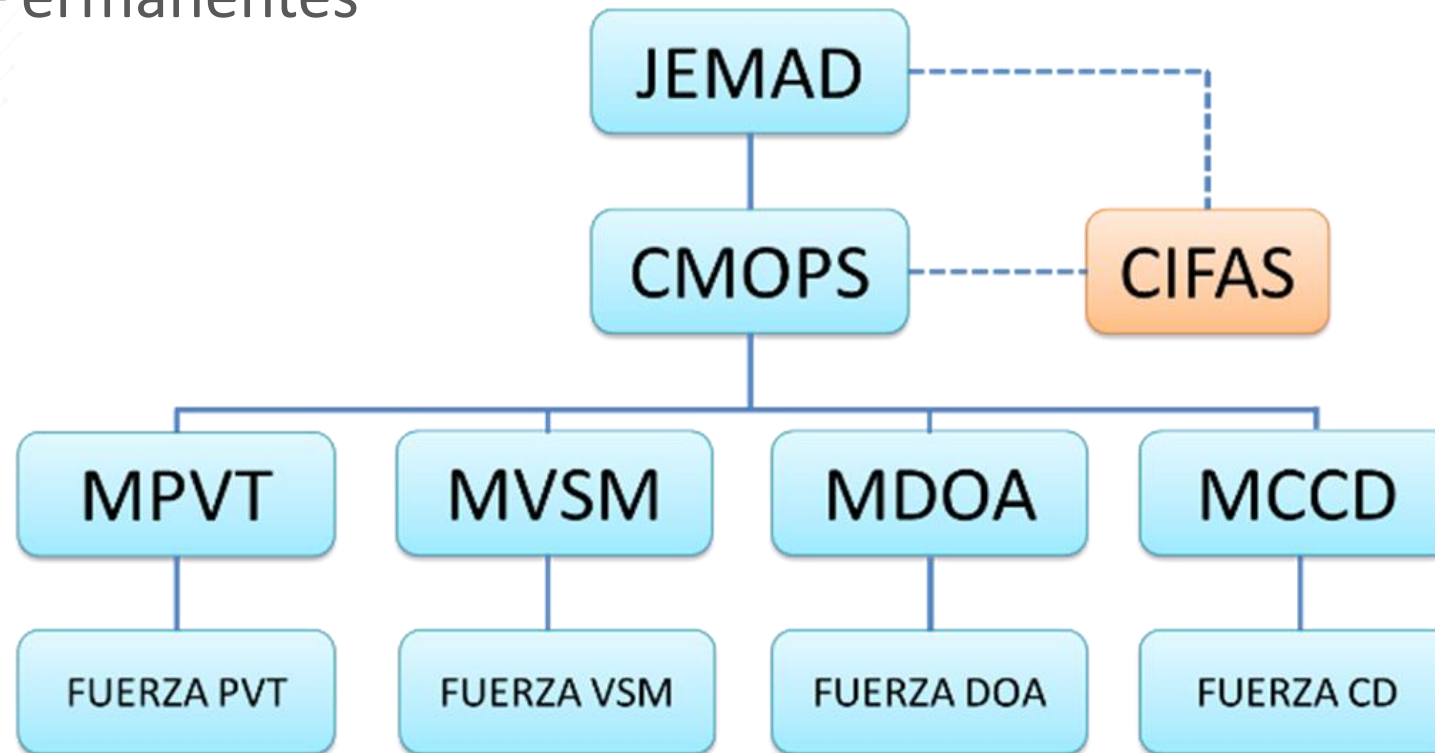


— Dependencia Orgánica

..... OPCON

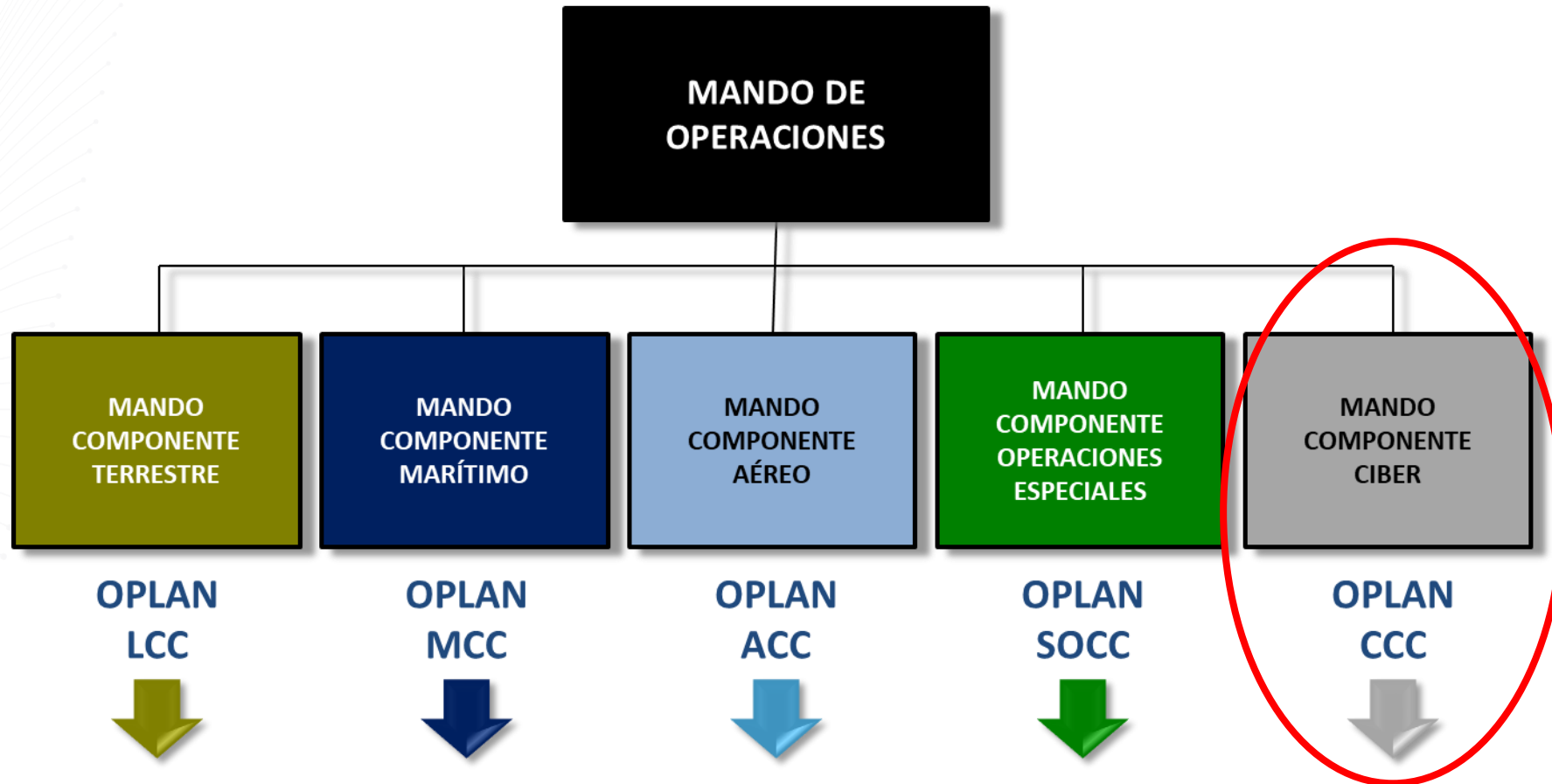
MCCD en la estructura conjunta de las FAS

Operaciones Permanentes



MCCD en la estructura conjunta de las FAS

Estructura operativa conjunta



OBJETIVOS OPERACIONALES

Conducción de operaciones

Conducción de operaciones

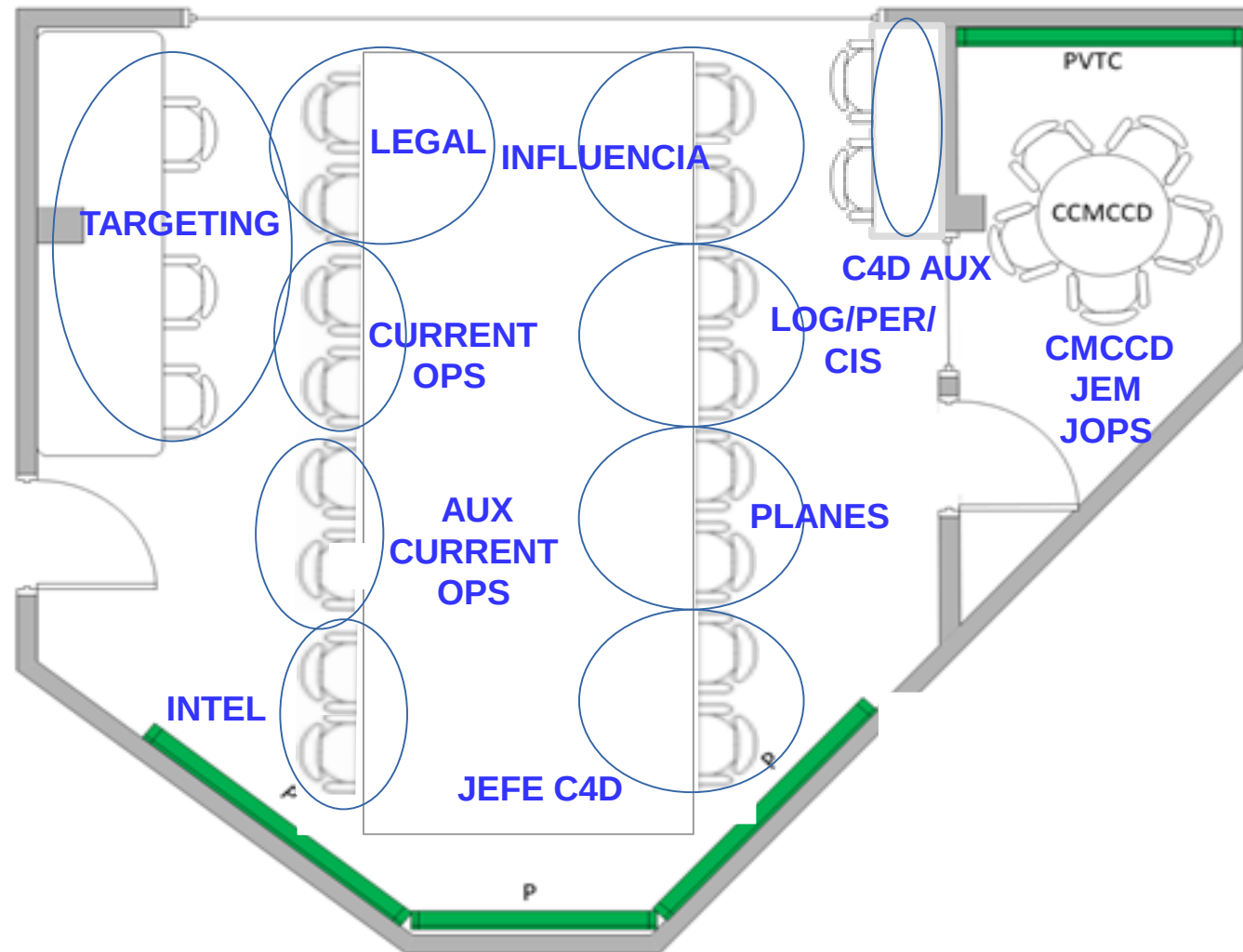
C4D: Centro de Control y Coordinación de Ciberdefensa

- **Conducción y control** de las **operaciones en el ciberespacio**.
- **POC** al nivel **operacional** con otros organismos (nacionales e internacionales).
- **Activado** para **operaciones** reales y ejercicios.
- Amplio **espectro** de **sistemas de C&C** (nacionales y OTAN).
- VTCs seguras para Operaciones Militares y con Estructura de Seguridad Nacional.
- Puestos: Ops en Curso, Planes, Inteligencia, Targeting, Legal, Logística y STRATCOM.



Conducción de operaciones

C4D: Centro de Control y Coordinación de Ciberdefensa

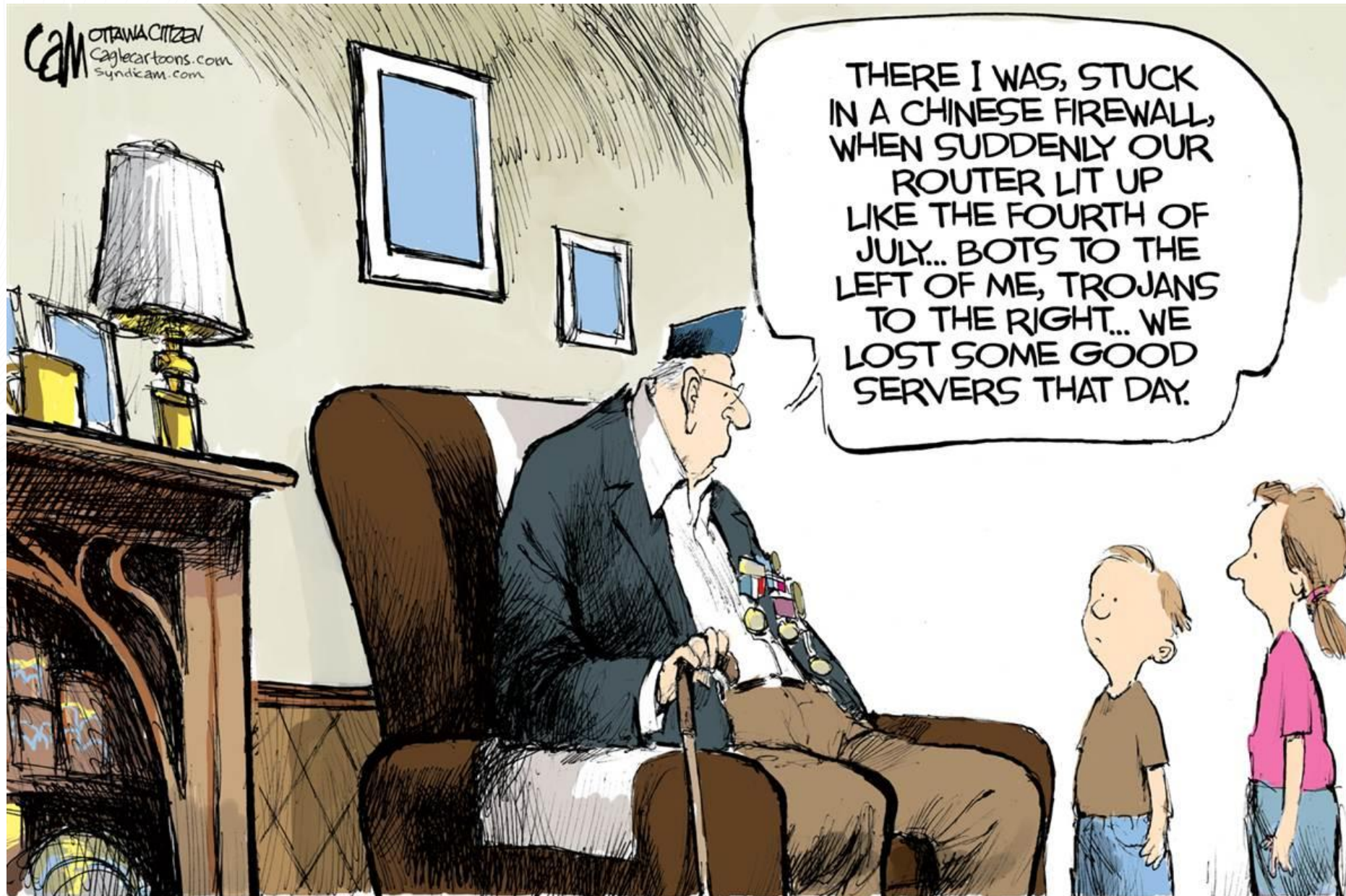


Conducción de operaciones

Operaciones de ciberdefensa dentro de un JOC conjunto

- **Operaciones en el ciberespacio NO** están integradas dentro de **J6** y las no son responsabilidad de J6.
- El **Cyber ops officer** debe estar integrado en J3 / J5, al igual que el resto de los oficiales de las operaciones terrestres, navales, áreas y especiales.
- En la “**PDC-03 Doctrina de Operaciones**” las operaciones en el ciberespacio es un tipo de operación más.
- Células Ad-hoc planeamiento operaciones en el ciberespacio (J3, J2, J5, J6).
- Oficiales de enlace en el restos de Mandos Componentes.
- Augmentees.





FUTURE WAR STORIES



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional