Mando Conjunto de Ciberdefensa

Teniente Coronel Manuel Saz Baselga

cyber camp
CYBERSECURITY EVENT
2016

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
TRABAJANDO POR LA CONFIANZA DIGITAL

CyberCamp.es

Ciberespacio
¿nuevo campo de batalla?

CARACTERISTICAS DEL CIBERESPACIO

Entorno virtual sin límites geográficos

Escasa seguridad

Se desarrollan actividades vitales para la sociedad -> hiperdependencia

Delincuencia, terrorismo y espionaje

Conflictos Armados

No control armamentístico

Anonimato vs Marco Legal

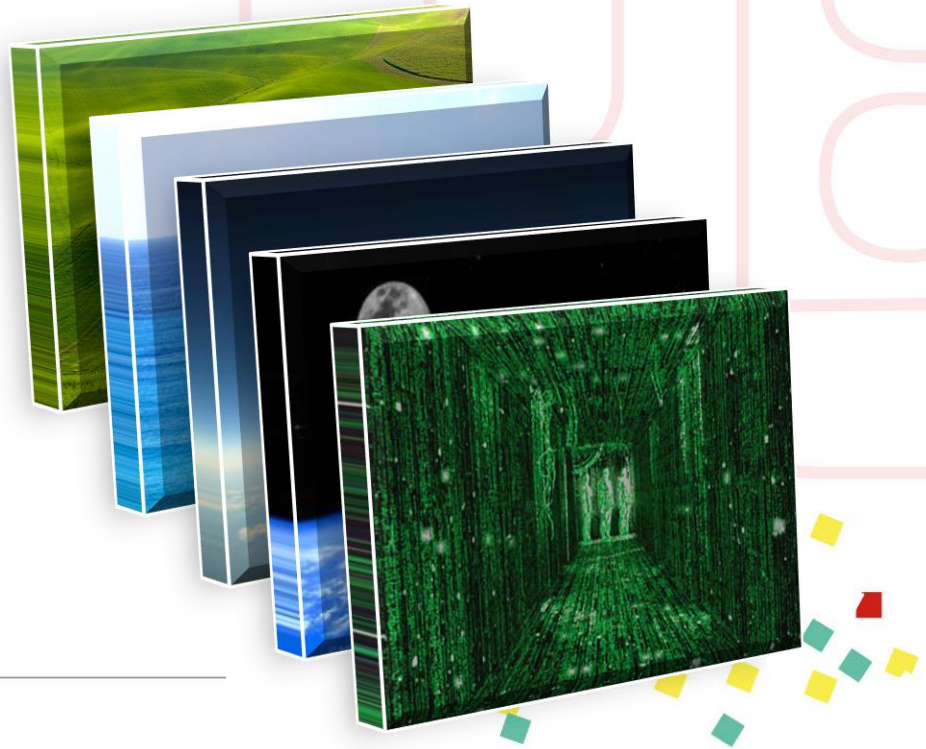
DEFINICION DE CIBERESPACIO

- **NATO Cyber Defence Taxonomy and Definitions (2014):**
  - Dominio global formado por los sistemas TIC y otros sistemas electrónicos, su interacción y la información que es almacenada, procesada o transmitida por estos sistemas.

GUERRA vs CIBERGUERRA

- **Guerra es la lucha armada entre dos o más naciones o entre bandos de una misma nación.**

- **Escenarios de las acciones armadas:**
  - Espacio Terrestre.
  - Espacio Marítimo.
  - Espacio Aéreo.
  - Espacio Exterior.
  - Ciberespacio.

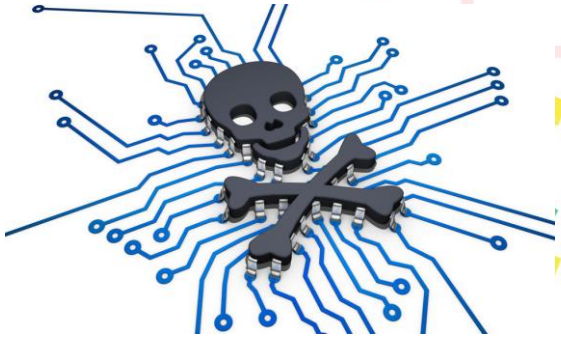


Amenazas en el Ciberespacio

AMENAZAS EN EL CIBERESPACIO

AMENAZAS EN EL CIBERESPACIO

- **Estados:**
  - Amenaza más peligrosa: acceso a recursos, personal y tiempo.
  - Conducen operaciones directamente o a través de terceros.
- **Actores Transnacionales:**
  - Organizaciones formales o informales no ligadas a fronteras nacionales.
  - Pueden ejercer "hacktivismo" o acciones terroristas haciendo uso del ciberespacio.



AMENAZAS EN EL CIBERESPACIO

- **Organizaciones criminales:**
  - No sujetas a fronteras.
  - Objetivo: ganancia económica.
  - Pueden prestar servicios a estados o actores transnacionales.

- **Actores individuales o pequeños grupos:**
  - Diversas motivaciones.
  - Pueden prestar servicios al resto de organizaciones.

ASIMETRIA DE ACTORES

Bajo coste ciberarmas

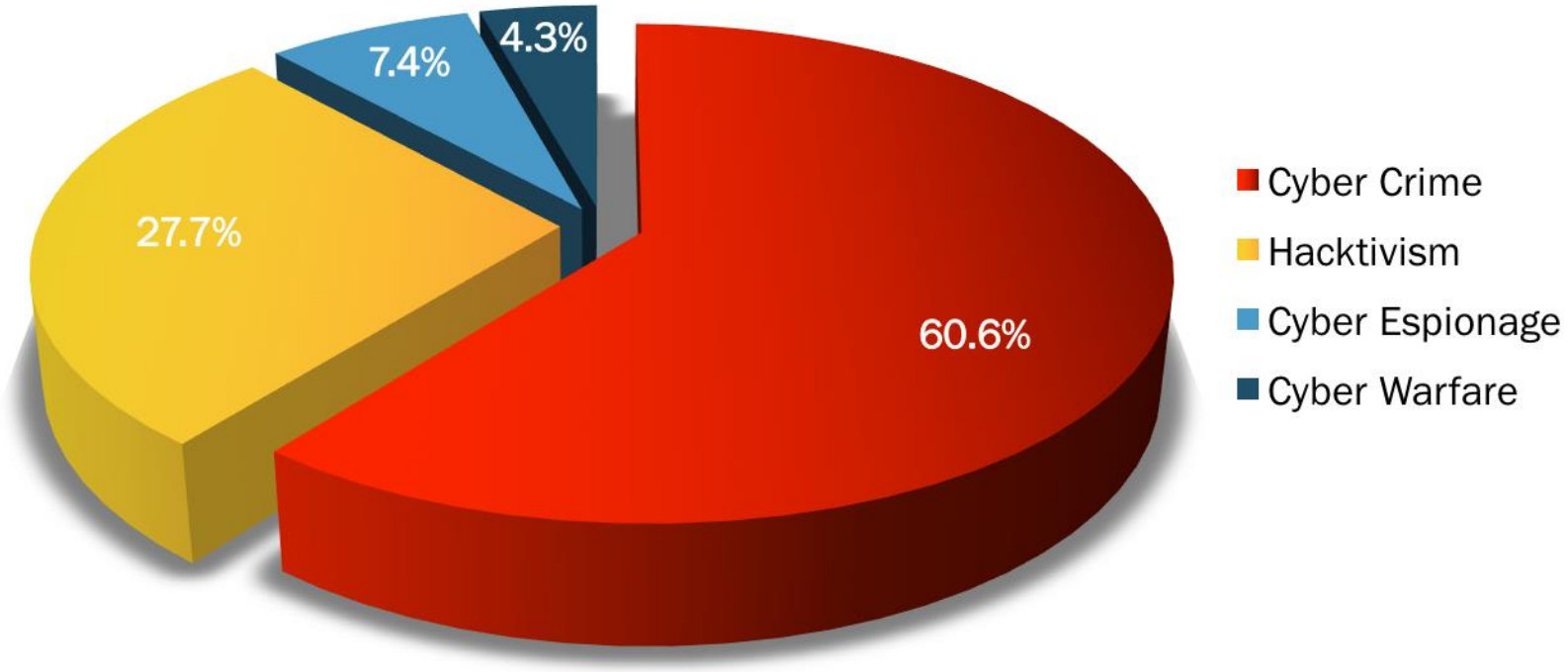
+

Elevada Eficacia

=

Asimetría

DISTRIBUCION DE LOS ATAQUES



Fuente: TrendMicro (Enero 2016)

Cometidos y Capacidades del Mando Conjunto de Ciberdefensa

COMETIDOS MCCD

- **RD 872/2014 (Organización FAS):**
  - Acciones de ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas.
  - Respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la Defensa Nacional.

CAPACIDADES MCCD

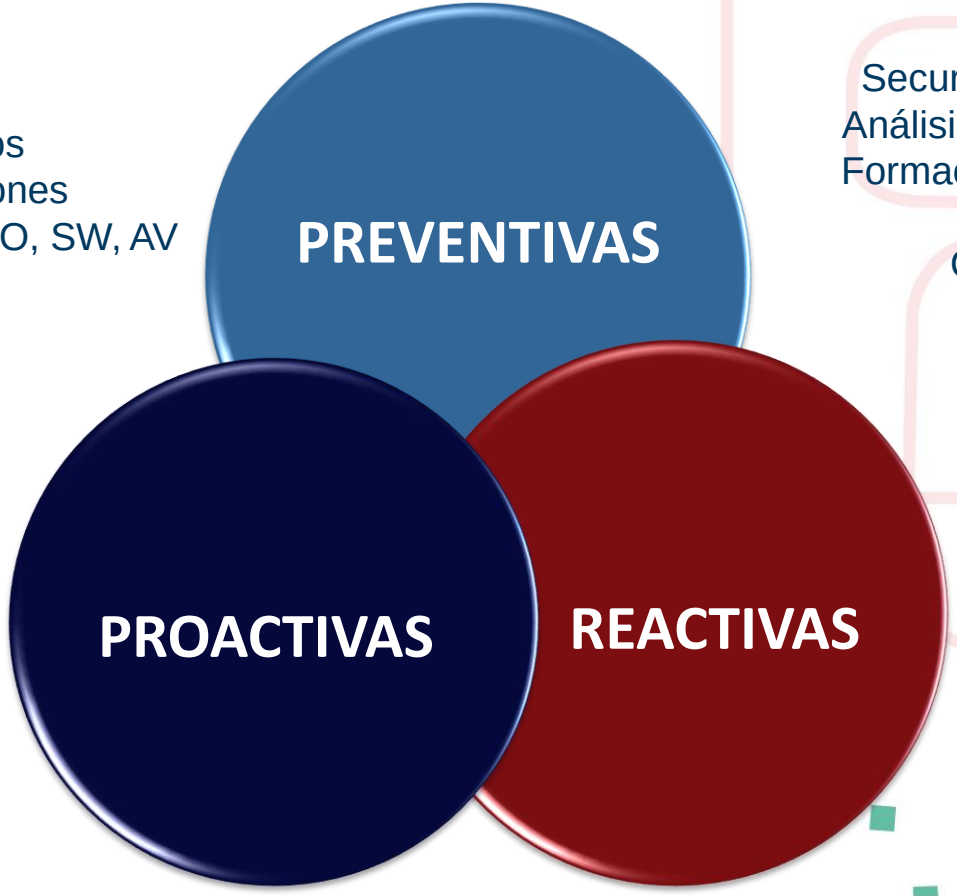
DEFENSA
PREVENTIVA
PROACTIVA
REACTIVA

EXPLOTACIÓN
CONOCIMIENTO SITUACION
INTELIGENCIA
ALERTA TEMPRANA

RESPUESTA
LEGÍTIMA
OPORTUNA
PROPORCIONADA

CAPACIDADES DE DEFENSA

Seguridad física
Control de accesos
Control de emanaciones
Actualizaciones HD, SO, SO, SW, AV



Securización de sistemas
Análisis de vulnerabilidades
Formación y Adiestramiento
Alertas
Concienciación

Inspecciones y Auditorías
Monitorización
Tests de penetración

Gestión de incidentes
Restauración de sistemas
Análisis forense
Atribución
Acciones legales

CAPACIDADES DE DEFENSA

SISTEMA

AOSTIC
(Autoridad Operativa)

AS
(Admin Segur)

Admin

SERVIDORES

Usuarios

CLIENTES

MCCD

APOYO TÉCNICO

MONITORIZACIÓN

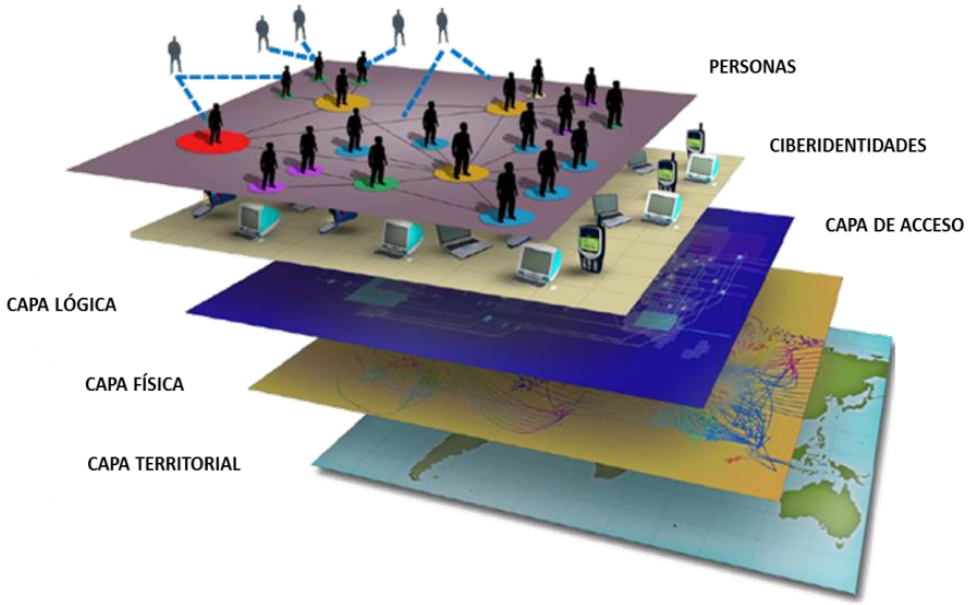
GESTIÓN DE INCIDENTES

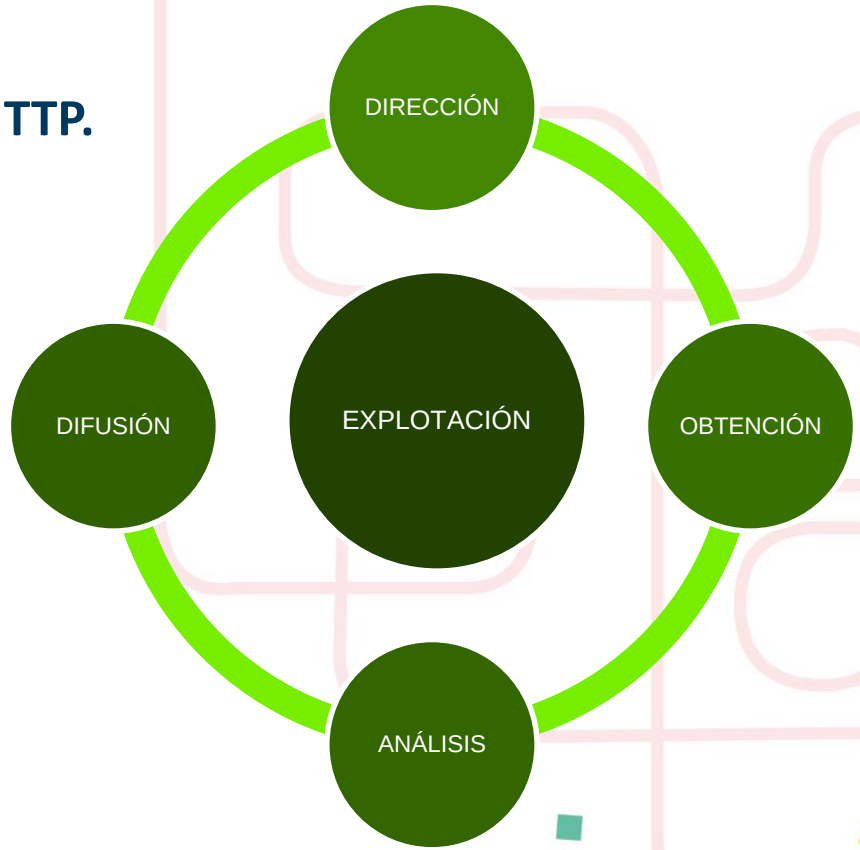
ERI

FORENSE

CAPACIDADES DE EXPLOTACION

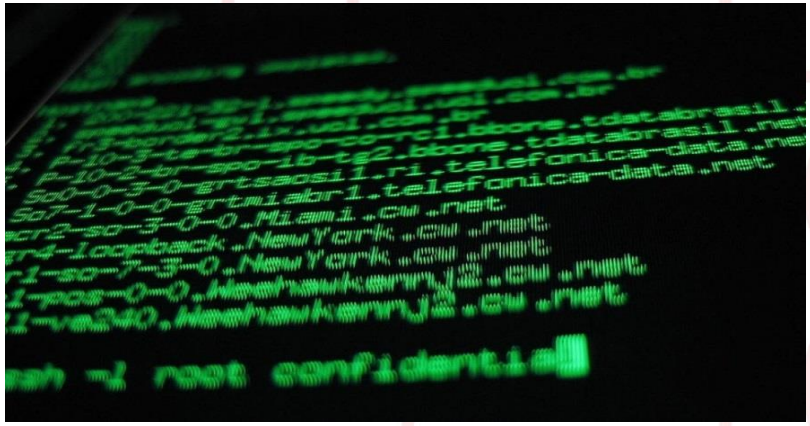
- **Inteligencia de ciberamenazas: ORBAT + TTP.**
- **Alerta temprana ante posibles ataques.**
- **Apoyo al Planeamiento de Operaciones.**





CAPACIDADES DE RESPUESTA

Acciones contra potenciales adversarios o agentes hostiles que afecten a la integridad y disponibilidad de sus sistemas de información y telecomunicaciones, así como a la información que éstos manejan.

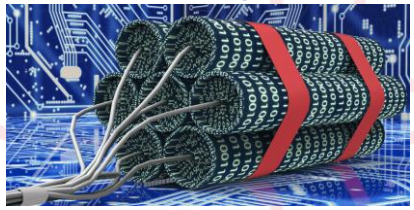


Operaciones Militares en el Ciberespacio

DEFINICIONES

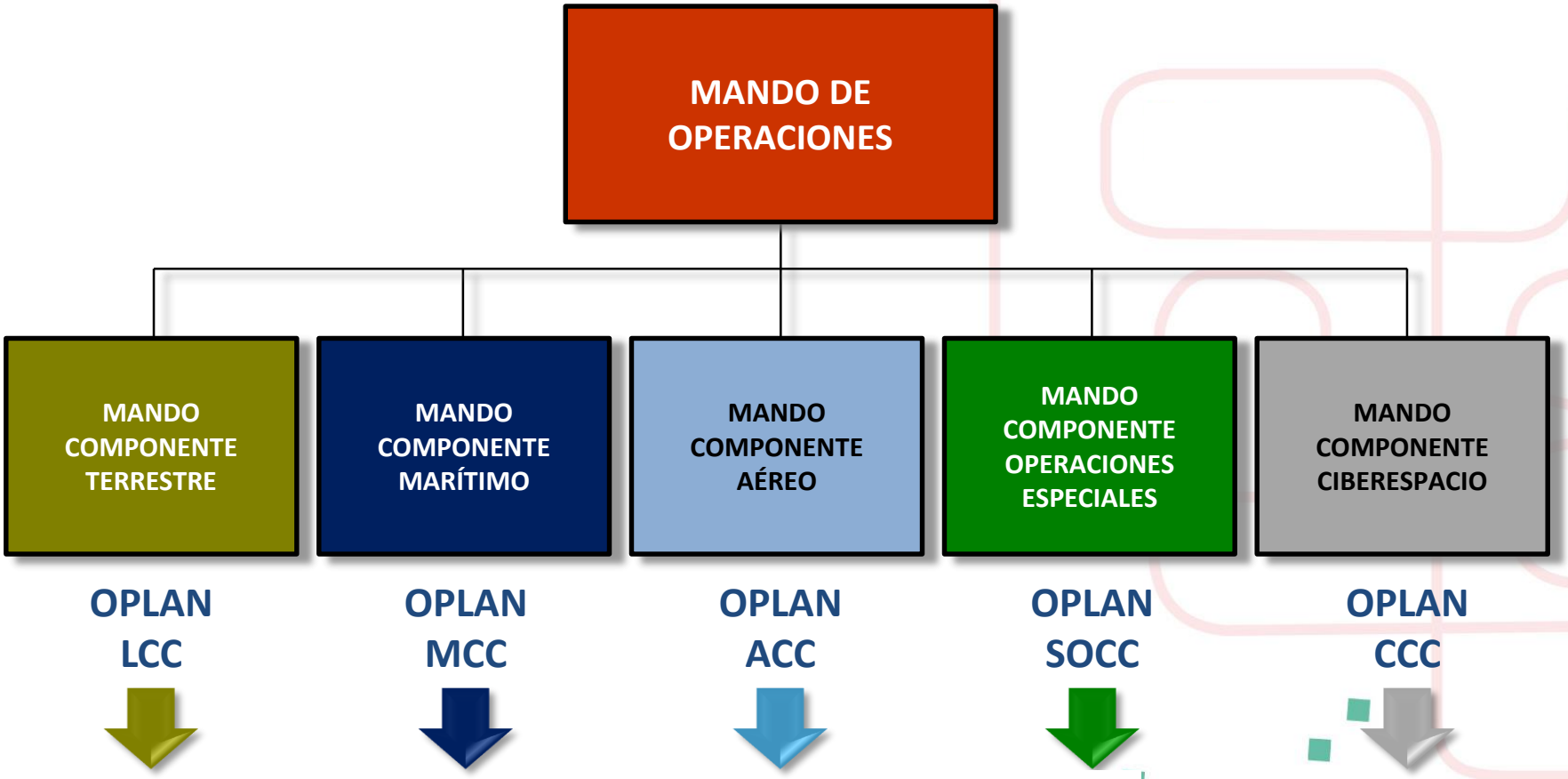
- **Operación Militar en el Ciberespacio:**
  - Es una operación en la que se emplean capacidades "ciber" con el objetivo principal de alcanzar objetivos militares en el ciberespacio o a través de él.

- **Ataque Armado en el Ciberespacio:**
  - Es una acción originada en el ciberespacio en la que se producen daños a personas u objetos.



- **Efectos en el Ciberespacio:**
  - Efectos producidos sobre los sistemas de información que afectan a la Confidencialidad, Integridad o Disponibilidad de la información contenida en ellos.

ESTRUCTURA OPERATIVA CONJUNTA



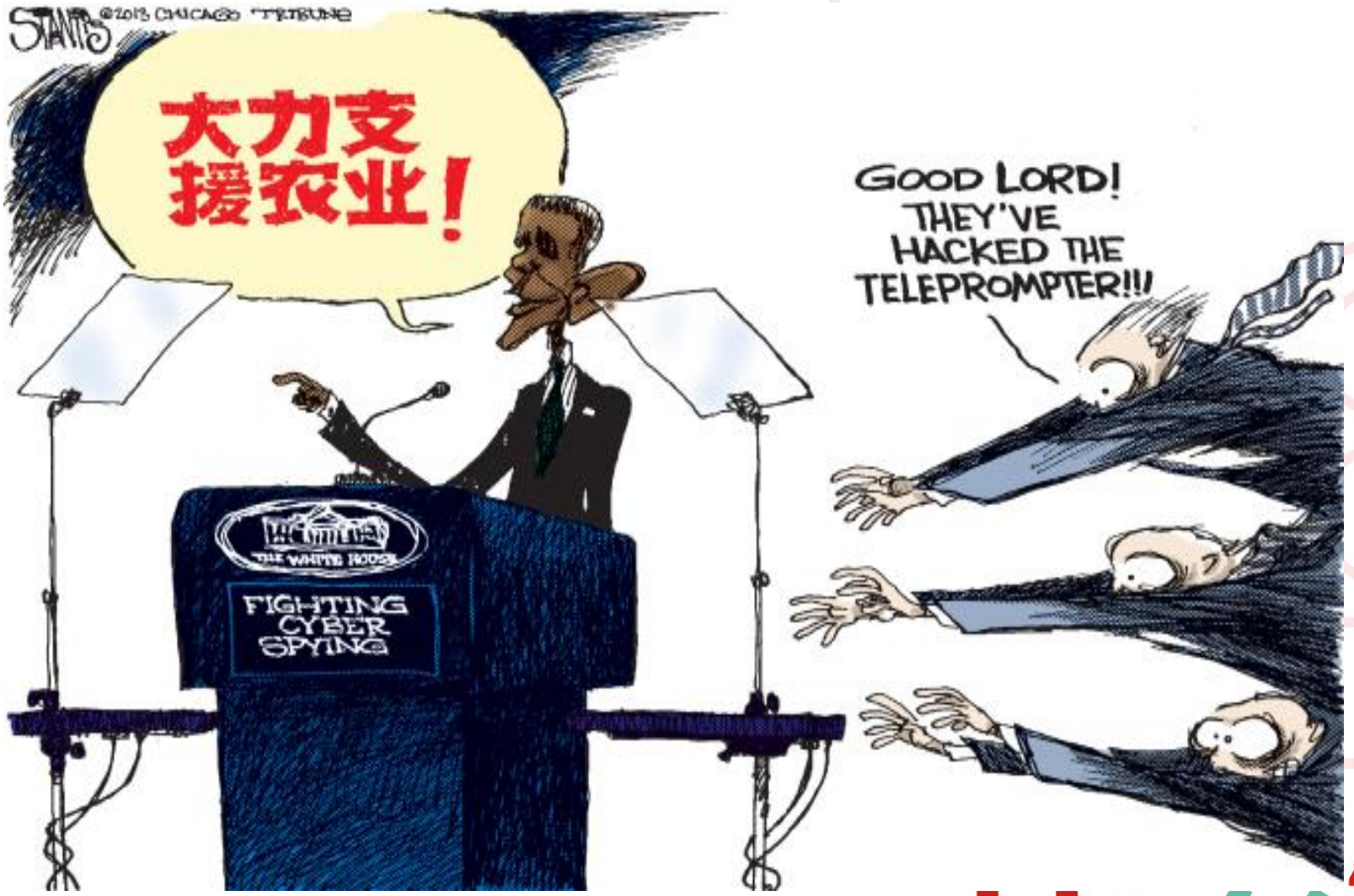
OBJETIVOS OPERACIONALES

AREA DE OPERACIONES DE CIBERDEFENSA (AOCD)

- **Área fija:**
  - Redes y sistemas TIC:
    - Del Ministerio de Defensa en territorio nacional.
    - En despliegues FAS en operaciones en el exterior.
    - Que se le encomienden.

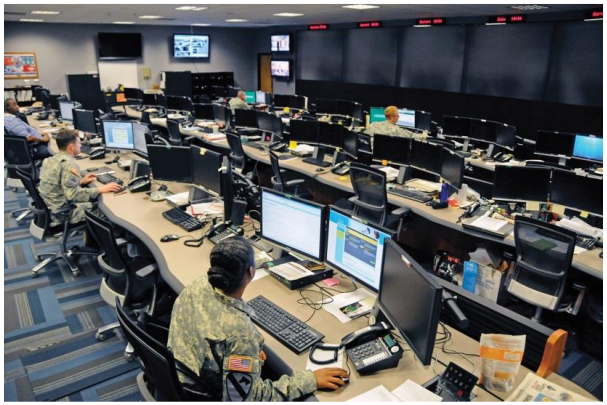
- **Área variable:**
  - Parte del ciberespacio de interés militar necesaria para:
    - Desarrollar una operación militar específica.
    - Responder a amenazas o agresiones que puedan afectar a la Defensa Nacional.

SUPERFICIE A DEFENDER



PLANEAMIENTO DE OPERACIONES EN EL CIBERESPACIO

- Las operaciones en el ciberespacio se planean igual que en el resto de dominios.

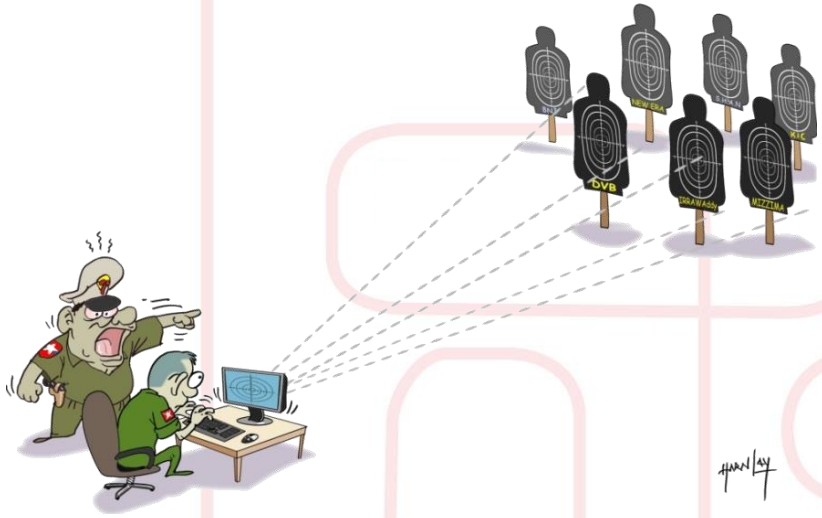


- Las acciones en el ciberespacio se deben integrar en todas las operaciones a nivel táctico, operacional y estratégico.

PLANEAMIENTO DE LAS OPERACIONES

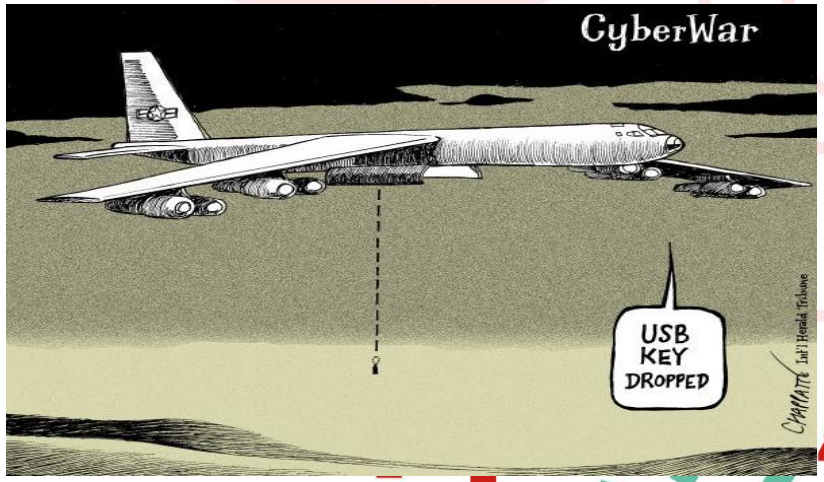
Cyber Targeting

Proceso de selección y priorización de objetivos en el ciberespacio, así como los efectos a producir sobre ellos.



Cyber Weaponeering

Proceso para determinar la cantidad y tipo de ciberarmamento necesario para producir los efectos deseados sobre un objetivo.



TIPOS DE OPERACIONES EN EL CIBERESPACIO

- **Operaciones Defensivas:**
  - Su objetivo es mantener la libertad de acción, evitando que se vea afectada la Confidencialidad, Integridad o Disponibilidad de la información.
  - Comprenden acciones para proteger, monitorizar, analizar, detectar y responder a actividades no autorizadas en sistemas de información propios.

  - Dos tipos:
    - Las realizadas permanentemente en los sistemas del Ministerio de Defensa (medidas de protección).
    - Las realizadas con misión de proteger un sistema específico contra una amenaza definida.

TIPOS DE OPERACIONES EN EL CIBERESPACIO

- **Operaciones de Explotación:**
  - Obtención de información de los sistemas adversarios designados como objetivos susceptibles de ser atacados.
  - Obtención de información del origen de ataques a sistemas propios.
  - Tipos:

    - Inteligencia de fuentes abiertas (OSINT): información DNS, Google hacking, sitios web y metadatos de archivos.
    - Reconocimiento pasivo: enumeración de dispositivos, escaneo de puertos activos (protocolos y servicios), identificación de SO,s y evaluación de vulnerabilidades.
    - Amenaza Persistente Avanzada (APT): exfiltración constante de información del objetivo mediante la penetración en sus sistemas.

TIPOS DE OPERACIONES EN EL CIBERESPACIO

- **Operaciones Ofensivas:**
  - Acciones realizadas en el ciberespacio para degradar, interrumpir, denegar o destruir sistemas de información o la propia información que estos almacenan.

  - Sincronizadas con acciones en otros dominios para alcanzar los objetivos militares asignados.
  - Requieren previamente de Operaciones de Explotación para la obtención de información.

CONTROL DE LAS OPERACIONES

Autoridad de Control del Ciberespacio

Autoridad que asume la responsabilidad del control de las operaciones en el AOCD.

Centro de Mando, Control y Conducción de CD (C4D)

Centro desde el cual se dirigen, controlan y ejecutan las Operaciones de Ciberdefensa.

Orden de Misión de Ciberdefensa (CTO)

Orden emitida por el CCD para la ejecución de acciones de ciberdefensa específicas o en apoyo a otros Mandos Componentes.


CYBERDEFENSE

2nd InService Brotherhood Bootcamp
Chulachomklao Royal Military Academy
Nakornnayok Province, Thailand
25-30 March 2008

MISSION ORDER

ARE YOU READY?!!!

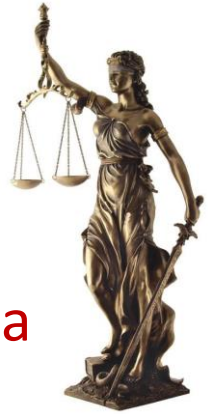
Based on your Application & Recommendation, you are hereby CONFIRMED by The V to PARTICIPATE and QUALIFY in the 2nd ISB Bootcamp.

Registration opens at 1400hrs and closes at 1800hrs on 25th March, at the RONG NON PAN ROR. CRMA (Chulachomklao Royal Military Academy)
Balance Payment: USD 250 CASH payment on site please present this

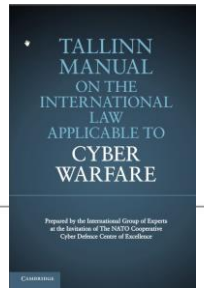
Legislación aplicable a las Operaciones en el Ciberespacio

MARCO LEGISLATIVO

- **Los Tratados Internacionales en vigor se aplican al ciberespacio (White House Cyber Strategy).**
  - Se aplican en tiempo de paz y en conflicto armado.
  - No existen tratados específicos para el ciberespacio.
  - Tallinn Manual: "Legislación internacional aplicable a la ciberguerra" (CCDCOE).



- **Soberanía: los Estados pueden ejercer el control sobre las "ciber-infrestructuras" y actividades dentro de su territorio soberano. (Tallinn Manual).**



CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

incibe_ TRABAJANDO POR LA CONFIANZA DIGITAL

JUS AD BELLUM

- **Marco legislativo nacional:**
  - Código Penal (España):
    - Acceso no autorizado a sistemas de información.
    - Interrupción no autorizada del funcionamiento de un sistema de inf.
  - Tanto en el país de origen, los de paso, como el de destino final del ciberataque.

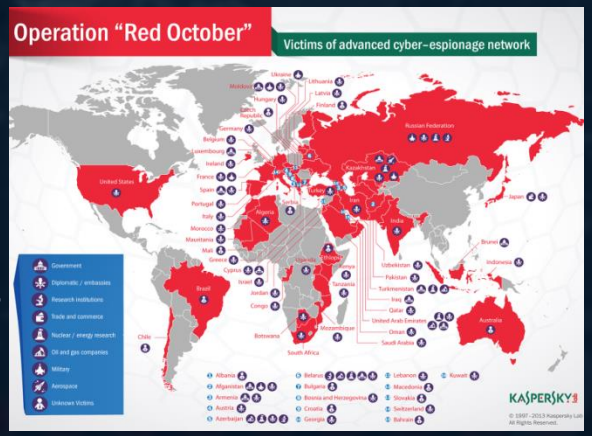
- **Derecho internacional:**
  - Prohíbe el uso de la fuerza, excepto en dos supuestos:
    - CSNU: para mantener y restaurar la paz y seguridad internacional.
    - Carta NNUU (Art 51): reconoce el derecho del uso de la fuerza en autodefensa en caso de ataque armado.

JUS IN BELLUM

- **Principios del Derecho Internacional Humanitario que regulan uso de la fuerza en conflictos armados:**
  - Distinción:
    - Exige la **discriminación** entre objetivos **militares y civiles**.
  - Proporcionalidad:
    - Se prohíben armas y métodos que causen **daños excesivos** con respecto a la **ventaja militar** esperada.
  - Necesidad militar:
    - Toda acción ha de responder a una **necesidad militar justificada**.
  - Humanidad:
    - Acciones contra objetivos militares, **preservando la vida** de la población e infraestructuras civiles.

OPERACIONES REALES

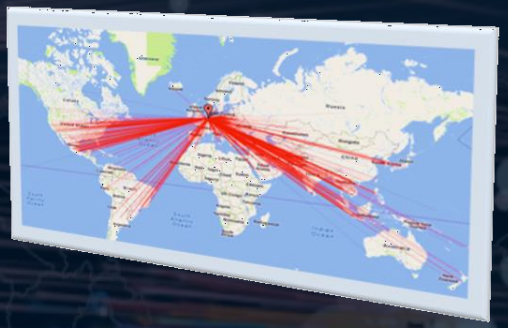
- Red October (2007-….):
  - Tipo de operación: ofensiva.
  - Objetivo: agencias diplomáticas y gobiernos de todo el mundo.
  - Efectos:
    - Exfiltración de información.
  - Vector de ataque: phishing e-mail.
  - Tipo de ataque: ciberespionaje.



R3D OCTOB3R

OPERACIONES REALES

- Estonia (2007):
  - Tipo de operación: ofensiva.
  - Objetivo: activos en la red de la administración del estado en Estonia.
  - Efectos:
    - Denegación de servicio.
    - Creación Centro de Excelencia de Ciberdefensa OTAN.
  - Vector de ataque: botnets a través de más de 170 países.
  - Tipo de ataque: cibersabotaje.



OPERACIONES REALES

- Buckshot Yankee (2008):
  - Tipo de operación: ofensiva / defensiva.
  - Objetivo: Departamento Defensa US.
  - Efectos:
    - Exfiltración de información.
    - Creación US CyberCom.
  - Vector de ataque: memoria USB “abandonada” en un parking.
  - Tipo de ataque: ciberespionaje.

OPERACIONES REALES

- Georgia – Osetia del Sur (2008):
  - Tipo de operación: ofensiva.
  - Objetivo: activos en la red de la administración del estado en Georgia.
  - Efectos:
    - Denegación de servicio.
    - Desvío de tráfico a través de otros servidores.

  - Vector de ataque: botnets y toma de control de servidores.
  - Tipo de ataque: ciberataque dentro de conflicto armado (previo a una ofensiva) = Ciberguerra.

OPERACIONES REALES

- Irán (2010):
  - Tipo de operación: ofensiva.
  - Objetivo: instalación nuclear en Irán.
  - Efectos:
    - Mal funcionamiento centrifugadoras de una planta de enriquecimiento de uranio.
    - Retraso de dos años del programa nuclear iraní.
  - Vector de ataque: memoria USB infectada (Stuxnet).
  - Tipo de ataque: cibersabotaje.

Gracias por su atención

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL