

XIII JORNADAS STIC CCN-CERT



Ciberlitoral



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

#XIIIJORNADASCCNCERT



CN José Ramón Brandariz Calviño

Jefe del Grupo e Ciberdefensa de la Armada

Armada Española / Ministerio de Defensa

DESCARGO DE RESPONSABILIDAD.

Lo expuesto en este documento representa exclusivamente las opiniones del autor. No constituye doctrina, ni postura oficial, de la Armada Española o del Ministerio de Defensa.

DISCLAIMER.

The views, thoughts, and opinions expressed in the text belong solely to the author, and not necessarily to the Spanish Navy or to the Spanish Ministry of Defence.

Índice

1. De la realidad a los conceptos.
2. “símbolos hidráulicos” y otros artificios.
3. El Ciberlitoral. (*“Los ciberlitorales”*)
4. Conclusiones.

De la realidad a los conceptos

Analogías como herramientas para facilitar la comprensión de la realidad



- El ser humano necesita entender la realidad (filosofía; ciencia; religión; artes)
- El ciberespacio es una nueva realidad *virtual* (contradicción) con relaciones con el mundo físico (real) y cognitivo (también virtual)
 - (definición) **Real**: Que tiene existencia objetiva [RAE]
 - En esta nueva realidad, construcción humana, también se materializan **conflictos** que afectan a los entornos físico y cognitivo.
 - El objetivo final de las guerras, uno de cuyos componentes pueden ser las operaciones militares, es siempre la voluntad de un adversario (vencer y/o convencer) [físico/virtual]
- Para ayudar a comprender el ámbito de las operaciones militares en el ciberespacio nos apoyaremos en la *analogía* del *ciberlitoral*.
- **Espacios de transición entre los dominios** (ámbitos) físicos: en el caso marítimo hablamos de **litoral**:
 - Perteneciente o relativo a la orilla o costa del mar [RAE]
 - En las operaciones navales el litoral tiene un tratamiento específico, que no es objeto de esta presentación.
 - “Franja” que comprende parte de la tierra y del mar contiguos. (no es una frontera / línea)
 - Fuerzas diseñadas para operar en el litoral: Infantería de Marina; Buques de Desembarco; LCS; etc
 - Espacio marítimo-terrestre; aguas poco profundas; estrechos; proyección de poder naval sobre tierra; bloqueos; puertos; islas;...

De la observación de la realidad, a la abstracción

El ciberespacio no se “siente” (no se ve...); cuando los sentidos no nos permiten objetivar una realidad (ej., campos eléctricos) recurrir a analogías puede ayudar a explicar algunos de sus aspectos.



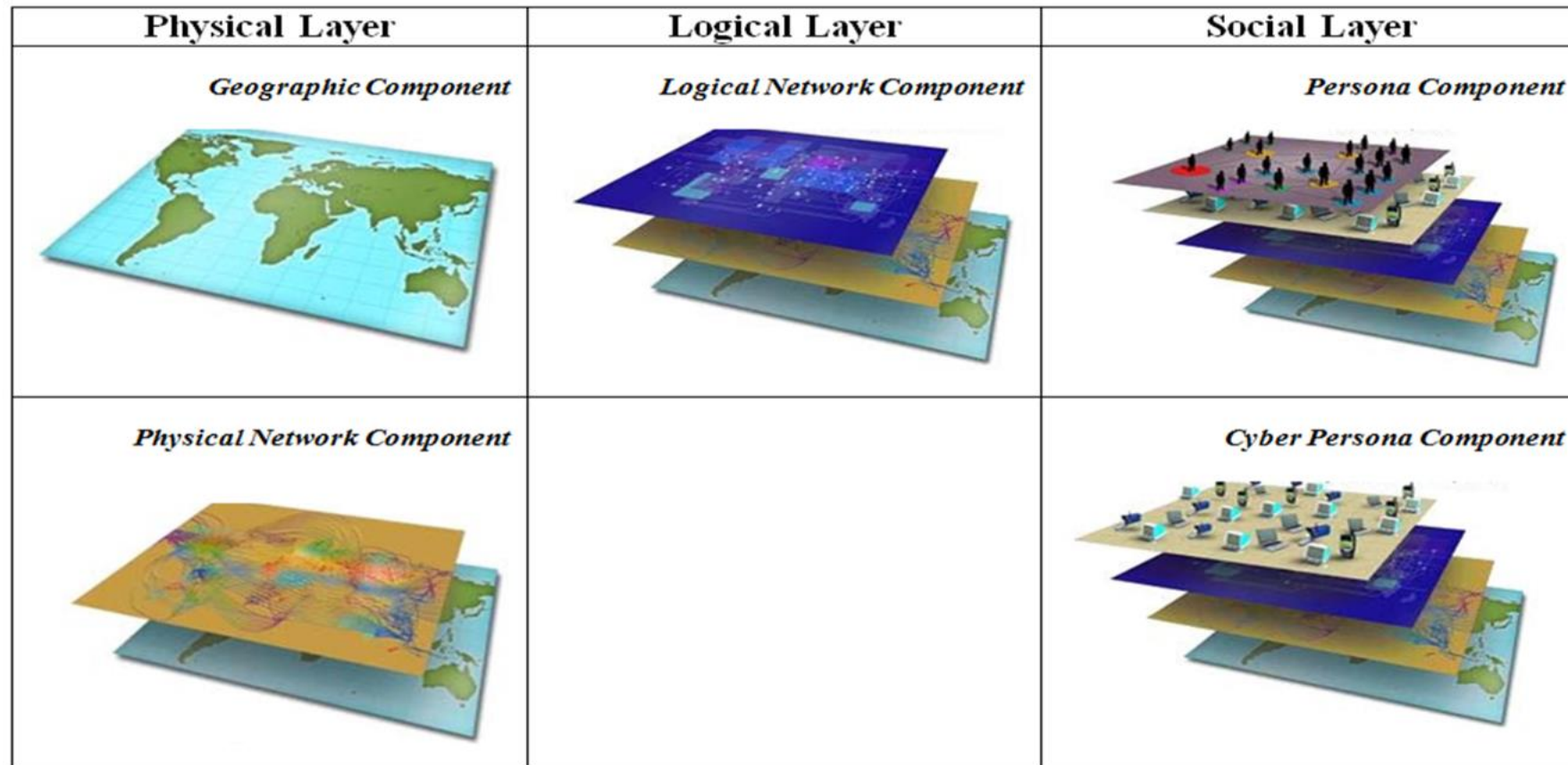
- Para explicar la electricidad con frecuencia se recurre al “simil hidráulico” (*líquido circulando a través de tuberías –conductores-; diferencias de potencial; resistencia; etc*)
- *Los ámbitos físicos (tierra, mar, aire, espacio) presentan áreas de solape (continuidad).*
- En el **ciberespacio**, para ayudar a definir el **ámbito** de las operaciones y, por tanto, para determinar las **capacidades necesarias**, se empleará el concepto de **ciberlitoral**.

Wikipedia. La **analogía eléctrico hidráulica** (conocida despectivamente como la *teoría de los desagües* por el físico británico Oliver Joseph Lodge (1851-1940)) es un procedimiento utilizado para simular mediante dispositivos hidráulicos el comportamiento de la *corriente* en un circuito eléctrico.

(Si se llevan demasiado lejos, las analogías pueden llevar inducir conceptos erróneos)

El Ciberespacio y su Paralelismo marítimo

AOCD = JOA
Área de Operaciones
de Ciberdefensa



CIBERLITORAL FISICO

SENSORES & ACTUADORES
(Robots y autómatas), IoT,
Cables submarinos, Cámaras CCTV
ESPECTRO ELECTROMAGNÉTICO
Satélites, GNSS, CEMA, EW, HW,
Centros de Datos, SCADA, OT, etc

CIBERESPACIO ABIERTO

Espacio principal de la maniobra táctica.

Alta mar (BGP, DNS, IXP,
Internet, cifra, **tiempo...**)
Cabotaje (LAN, CIS, SW)

CIBERLITORAL SOCIAL y COGNITIVO

OSINT,
INFLUENCIA
Personas, **Grupos**, enlaces
CiberIdentidades

Los conocimientos y adiestramiento (“aptitudes”) de los cibercombatientes no se deben de limitar a CONOCER Y DOMINAR LA MANIOBRA CIBERTÁCTICA, deben ser capaces de usar el ciberespacio tanto para proyectar fuerza sobre los demás dominios como para dominar el CIBERESPACIO de interés.

CIBER-SUPREMACÍA

CIBER-SUPERIORIDAD LOCAL

CIBER-CONTROL LOCAL

CIBER-CONTROL LOCAL-TEMPORAL

Etc

Imprescindible mantener la CySA

(CySA) CYBER SITUATIONAL AWARENESS

Redes aisladas son como Mares cerrados o protegidos por un estrecho:

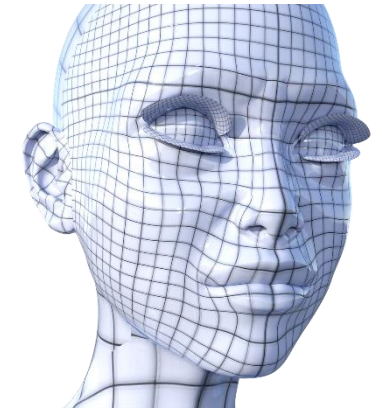
CIBERDESEMBARCO (ciberintrusión)

CONCLUSIONES

Las capacidades militares en el ciberespacio han de adaptarse a su realidad.

1. El ciberespacio “toca” al mundo físico y al cognitivo en múltiples “superficies”:

- Espectro electromagnético (SDR; control de telecomunicaciones; EW)
- Control de sensores y actuadores
 - Tecnología Operacional (OT) : Sistemas de control (ICS, SCADA, PLC, IoT, etc)
 - Tecnología de Información (IT) directamente asociada al control
- Vehículos autónomos. Enjambres de drones. (armas autónomas)
- Inteligencia Artificial. Big Data. Tecnologías de diseño asistido. Impresión 3D.
- Redes sociales; influencers; *fake-everything*; realidad virtual; etc
- Medicina y salud; etc



2. Las acciones en el ciberespacio tienen efectos en el mundo físico y en el cognitivo.

- Necesario contar con una visión general que abarque suficientemente todos estos aspectos (*Cyber Situational Awareness*). Saber qué está pasando. Ciberinteligencia.
- Necesario contar con medios y personas para contrarrestar, en el ciberespacio y en los ciberlitorales, los efectos que el adversario quiera causar para perjudicar los intereses nacionales.
- El necesario control centralizado de las ciberoperaciones no ha de impedir las acciones tácticas en el ciberespacio en apoyo de una operación convencional. Toda misión convencional tendrá aspectos ciber y el comandante debe contar con cibercapacidades orgánicas al nivel necesario que se determine.



XIII JORNADAS STIC CCN-CERT

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

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

CCN-cert
centro criptológico nacional