LOS LITORALES DEL CIBERESPACIO

José Ramón BRANDARIZ CALVIÑO

(reserva)

En el ciberespacio, más que en cualquier otro ámbito, el que no avanza rápido retrocede.

(Del autor)

Introducción

L ciberespacio (CE) es un ámbito artificial en donde se materializan conflictos que afectan a los entornos físico y cognitivo. Los conflictos son una constante en la condición humana y el objetivo final de la política (la eterna lucha por el poder), es siempre doblegar la voluntad del adversario; cuando la política se torna más violenta, continúa a través de la guerra (1), pero el objetivo sigue siendo el mismo: vencer y/o convencer (físico y/o virtual); existen muchas formas de lograrlo: persuadir, disuadir, influir, reclutar, atraer, engañar, comprar, sobornar, someter, obligar, convertir, juramentar, adoctrinar, reeducar, alienar… o encerrar en una matrix. Pero el principio básico fundamental se mantiene: vencer/convencer *(hard/soft),* y en la aplicación de ese principio, hoy en día, no cabe duda de que el ciberespacio juega un papel primordial.

Históricamente se han usado analogías y símiles para entender o explicar la realidad. Así, el «símil hidráulico», usado para explicar la corriente eléctrica, equiparaba el funcionamiento de la energía eléctrica con el de un fluido moviéndose (corriente) en una tubería (conductor) debido a la acción de la

(1) CLAUSEWITZ, Carl von: *De la guerra*. «La guerra es la continuación de la política por otros medios». Ediciones del Ministerio de Defensa de España, dos volúmenes, 1999.

gravedad (diferencia de potencial) moviendo una turbina (resistencia). En este artículo trato de aplicar este artificio, haciendo un símil metafórico entre lo marítimo y lo ciberespacial para explicar lo que, a mi modo de ver, abarca el ciberespacio, sus límites y sus relaciones con los ámbitos físicos (tierra, mar, aire y espacio). Naturalmente, toda analogía es imperfecta y puede llevarnos a graves errores cuando se toma al pie de la letra. Véase, por tanto, este ensayo como una aproximación inicial que puede facilitar el conocimiento del ciberespacio y ayudar a deducir las características necesarias que ha de tener la fuerza encargada de proteger los intereses nacionales en este nuevo ámbito artificial.

¿Existe el ciberespacio? (2)

No pretendo responder a esta pregunta aquí y encomiendo al lector interesado a investigar por su cuenta en internet; hay opiniones (3) muy interesantes. Tan solo quiero decir que, independientemente de la respuesta, lo cierto es que el ciberespacio tiene efectos en nuestras vidas: en la economía y en la energía; en las comunicaciones y en las relaciones; en el comercio y en el transporte; en el ocio y en el arte; en general, en casi todos los aspectos de la vida moderna.

Habitualmente se representa el ciberespacio mediante una abstracción consistente en una serie de capas que supuestamente lo configuran: la capa física, la capa lógica y la capa social. La física tiene componentes geográficos (dónde se ubican los elementos físicos que componen la red) y los propios componentes de la red física (cableado, ordenadores, terminales de usuario, electrónica de red y otro *hardware*, además de sensores y actuadores que interaccionan con el mundo físico); la capa lógica abarca aquellos componentes que forman la red lógica (protocolos, datos, sistemas operativos, servicios y aplicaciones, sistemas de direccionamiento, el *software* en general y el *firmware*); y, por último, la capa social consta del componente «ciberpersona» (ciberpersonaje o rol que se «materializa» en el ciberespacio mediante una dirección de correo electrónico, un nombre de usuario, etc., junto con los grupos y relaciones en el mundo virtual) y del componente abstracto «persona» (4), el personaje o imagen

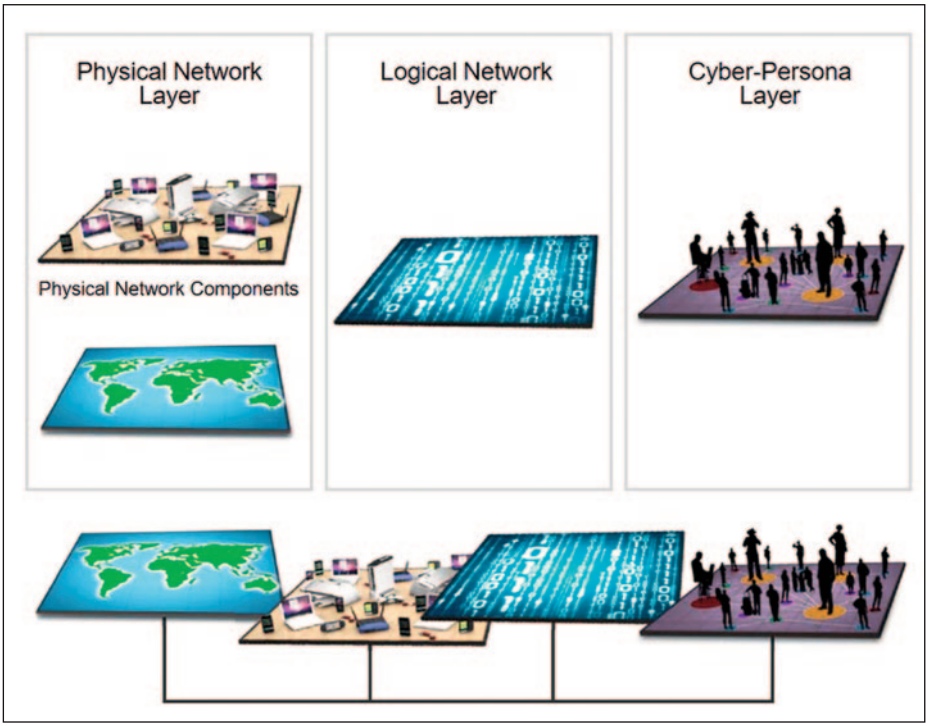
---

(2) El término ciberespacio (*cyberspace*) fue utilizado por primera vez por el escritor William Gibson en una publicación en 1982 y, posteriormente, en su novela de 1984 *Neuromancer* (*https://www.britannica.com/topic/Neuromancer*), consultado en julio de 2022.

(3) Dewar, Robert: «Cyberspace is a Consensual Hallucination», CSS ETH Zurich, *Policy Perspectives*, vol. 6/2, April 2018, *https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP6-2.pdf,* consultado en julio de 2022.

(4) Persona en inglés se traduce en español por «imagen pública» o «personaje de ficción»; no confundir con persona en español: «individuo de la especie humana» (RAE). Ver *https://csrc.nist.gov/glossary/term/persona*

pública que interpretamos delante del teclado, con una o muchas (5) «ciberpersonas» asociadas. Por fuera de la capa social del ciberespacio, pero profundamente influenciado por lo que ocurre en esta, se encuentra el individuo real («persona», en español) y sus grupos y relaciones sociales en el mundo físico. Precisamente esta influencia se aplica a través de lo que se denomina ámbito cognitivo.



Las tres capas interrelacionadas del ciberespacio.
(Imagen: «The Three Interrelated Layers of Cyberspace. (JP 3-12 Cyberspace Operations)»

(5) La relación entre ciberpersona, persona o individuo es de «muchos a muchos»: un individuo puede interpretar a múltiples personajes en el ciberespacio, y un personaje puede ser manejado por múltiples individuos. Lo mismo para la ciberpersona: una dirección de correo electrónico puede ser manejada por múltiples individuos, y un individuo puede tener muchas direcciones de correo electrónico, etc. El anonimato en el ciberespacio se sustenta en esta característica.

El litoral

El litoral (6) es un espacio de transición entre dos medios: el terrestre y el marítimo. Por analogía, podríamos decir que el ciberespacio tiene ciberlitorales con los ámbitos con los que interactúa. Como primera aproximación, habría al menos un ciberlitoral físico y otro social. Veremos a continuación que podemos identificar alguno más.

Para comprender mejor lo que abarcan las operaciones militares en el ciberespacio nos apoyaremos en esta analogía del ciberlitoral. Como se dijo anteriormente, cuando hablamos de espacios de transición entre los dominios (ámbitos) físicos, en el caso marítimo, hablamos de litoral. En las operaciones navales el litoral tiene un tratamiento específico.

Conviene tener presente que el litoral no es una línea, sino una «franja» que comprende parte de la tierra y del mar contiguos (que incluye el espacio marítimo-terrestre). Los límites de la franja litoral evolucionan con la tecnología y con el alcance de las armas.

La Armada cuenta con fuerzas diseñadas para operar en el litoral y proyectar el poder naval sobre tierra: la Infantería de Marina, los buques de desembarco,

Ciberespacio y su paralelismo marítimo

(6) Litoral: 1. adj. Perteneciente o relativo a la orilla o costa del mar. 3. m. Costa de un mar, país o territorio. *Diccionario de la lengua española*, 23.ª ed., versión 23.5 en línea, *https://dle.rae.es*, consultado en junio de 2022.

etc.; incluso se diseñan unidades específicas para el combate en el litoral (7) y en aguas poco profundas.

¿Quiere esto decir que, en el ámbito de las operaciones militares en el ciberespacio, la fuerza ciberespacial debería contar con componentes especializados en los ciberlitorales? Mi opinión es que sí y trataré de argumentarlo.

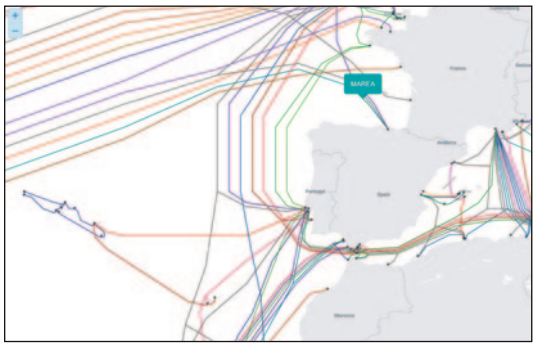
En la anterior figura se aprecia una visión general de las zonas del ciberespacio y sus ciberlitorales.

Litorales físicos

El ciberespacio «toca» al mundo físico en varias formas. Por un lado, le sirve literalmente de apoyo (geografía); por otro, interactúa con él mediante sensores y actuadores (detectando y moviendo cosas), sin olvidar que también interactúa con el entorno electromagnético (EME).

Aspectos geográficos

Componentes tales como los cables submarinos, las auténticas autopistas de la información que transportan el 99 por 100 del tráfico de datos intercontinentales, cruzan los océanos y tocan tierra en puntos muy concretos. Los grandes centros de datos se ubican en lugares especialmente protegidos. Los satélites de comunicaciones se sitúan en determinadas órbitas y sus estaciones de anclaje en tierra han de ser protegidas. Las redes de datos de fibra óptica se extienden por las ciudades y por todo el territorio. Las estaciones base de telefonía móvil se instalan en localizaciones óptimas para maximizar su rendimiento.



Cables submarinos.
(*https://www.submarinecablemap.com*)

Todos estos componentes físicos del ciberespacio son vulnerables, no solo a ciberataques, sino a acciones físicas sobre ellos, en función de su ubicación

(7) *Littoral combat ship* (LCS), *https://en.wikipedia.org/wiki/Littoral_combat_ship*, consultado en julio de 2022.

geográfica y de la amenaza, y deben, por tanto, ser protegidos. Los efectos de estos componentes sobre el medio ambiente y la actividad económica en la zona son también factores a considerar.

Actuaciones sobre el mundo físico. Sensores y actuadores

Sistemas de tecnologías de operación (TO o, en inglés, OT) —también conocidos como *cyber-physical systems* (CPS)— es la denominación genérica actual que comprende los sistemas de control industrial (SCI o ICS), los sistemas empotrados o —como se denominan en la Armada— integrados (*embedded systems*), las *platforms information technology* (PIT), etcétera.

Estos sistemas TO son gobernados hoy en día mediante tecnología digital y están conectados, directa o indirectamente, al ciberespacio.

De este modo, podemos decir que el CE interactúa con el mundo físico: captando señales, imágenes, parámetros, variaciones, datos… y actuando sobre él en diversas formas: construyendo herramientas, poniendo en marcha o deteniendo máquinas o fuentes de energía, controlando el transporte, dirigiendo drones, modificando el entorno o destruyendo objetivos mediante armas, lanzadas con ayudas a la decisión basadas en el CE y dirigidas por tecnología del CE.

Entorno y espectro electromagnético. EME y EMS (8)

La energía electromagnética juega un papel muy relevante para la existencia del CE, ya que a través del EME el CE «cobra vida» e interactúa con el entorno. Los campos eléctricos y magnéticos y las ondas EM posibilitan el procesamiento, almacenamiento y transmisión de datos e información. Por otro lado, gran parte del uso que se hace del EME se controla y gestiona a través del ciberespacio. Las formas de onda de radio se generan desde radios definidas por *software* (SDR, *Software Defined Radio*); las telecomunicaciones se basan en el transporte de datos aprovechando el EMS (ya sea en forma de luz o de otras ondas de radiofrecuencia). Los sistemas de guerra electrónica (9) (EW, *Electronic Warfare*) se controlan mediante *software*. Los sistemas actuales de posicionamiento (GNSS) y de identificación electrónica (AIS, IFF, etc.) también están basados en el EMS y en la tecnología digital, componentes básicos del CE. El entorno electromagnético es, evidentemente, parte del mundo físico, pero podemos identificar en él un ciberlitoral diferenciado del ciberlitoral físico, ya que tiene características propias. De hecho, ya se le presta una especial atención

(8) EME, *Electromagnetic Environment*. EMS, *Electromagnetic Spectrum*.
(9) Realmente deberían llamarse sistemas de guerra electromagnética.

militar mediante iniciativas como *Navigation Warfare* (NAVWAR), *Cyber Electromagnetic Activities* (CEMA) o el reconocimiento del espacio como dominio de enfrentamiento (fundamentalmente debido a los satélites artificiales que sustentan capacidades del EME, como SATCOM y GNSS, entre otros).

Litoral social y cognitivo

Aquí identificamos dos nuevos ciberlitorales muy relacionados entre sí: el social y el cognitivo.

«Persona», individuo, grupos y relaciones

Como vimos anteriormente, las ciberpersonas tienen su propia existencia virtual en el CE, ya sea controlada por mediación humana o por inteligencia artificial o automatismos (*bots*). Estas ciberpersonas y sus personajes asociados (avatares) tienen sus propias relaciones sociales virtuales agrupándose con otras de su misma naturaleza, sin estar sometidas a las limitaciones de distancia, fronteras o idioma. En este ciberlitoral social, el conocimiento del comportamiento, de las capacidades y de la dinámica de estos elementos y grupos y sus relaciones requiere de unas destrezas claramente diferenciadas con respecto a las necesarias en otras zonas del CE.

A través de la capa social, mediante la operativa de ciberpersonajes y grupos, se influye en las personas reales (individuos) y grupos sociales, atacando directamente al elemento cognitivo, distorsionando o modificando la percepción de la realidad y condicionando por tanto los comportamientos y las decisiones. Se trata del ciberlitoral cognitivo, que requiere de otras habilidades diferentes a las anteriores.

Inteligencia y ciberinteligencia en el ciberespacio

En la capa social del CE es donde se desenvuelve la información y la desinformación sobre el mundo real. Por tanto, es aquí donde la inteligencia en el CE tiene su principal campo de actuación, tanto la de fuentes abiertas (OSINT) como de otras (caso Pegasus, por ejemplo). Existe otra ciberinteligencia que se extiende más allá de la capa social por todo el CE y que se ocupa principalmente del propio CE. Está orientada a conocer las ciberamenazas (cibercapacidades, técnicas tácticas y procedimientos del adversario, así como a averiguar sus intenciones en el CE) y las vulnerabilidades del CE, ya sea para protegerse de su explotación contra los intereses propios por parte del adversario o para aprovecharlas en contra de él.

Ámbito cognitivo: desinformación, *fake news*, intoxicación informativa y medias verdades

La relación entre la capa social del CE y el ámbito cognitivo es evidente. El CE se usa como herramienta (arma) para modificar comportamientos mediante técnicas de desinformación, cibercensura sobre individuos o grupos disidentes, *fake news*, inundación con noticias irrelevantes para ocultar las importantes, aparición de verificadores pseudoindependientes a los que nadie ha verificado. Al fin y al cabo, lo que ha hecho siempre la propaganda, aunque ahora con un alcance y una potencia mucho mayores merced a la ubicuidad y la accesibilidad del CE, que facilita la aparición de cajas de resonancia (*echo chambers*) en donde se reúnen personajes con ideas afines, desterrando las demás y el debate constructivo, lo que produce una realimentación positiva que tiende a acentuar los extremismos.

El ciberespacio «abierto»

Entre las capas física y social de CE está la capa lógica. Aunque los litorales se encuentran fundamentalmente en aquellas, siguiendo el símil marítimo, en la capa lógica en donde podemos ubicar el mar abierto (CE abierto) con su navegación de altura —aquellos que se aventuran en las profundidades del *backbone* de internet, con sus sistemas autónomos (10), *root name servers* (DNS) (11), BGP, puntos neutros (IXP) (12), etc.— y su navegación de cabotaje —por las redes LAN, con sus servidores, *routers, firewalls*, puertos, protocolos, servicios y aplicaciones). Pero esto daría para otro «símil hidráulico».

Conclusiones

Las capacidades militares en el ciberespacio han de adaptarse a la nueva realidad del CE. Los ciberlitorales son un elemento clave (*Cyber Key Terrain*) (13) para la proyección de ciberfuerza: la defensa avanzada debe montarse en donde suceden las cosas: en los ciberlitorales físico y social-cognitivo.

Como se ha visto, el ciberespacio «toca» al mundo físico y al social-cognitivo en múltiples «superficies». No es realista pensar que existe un único tipo de ciberguerrero, una especie de *super cyberman*, que sea capaz de moverse con

---

(10) *https://en.wikipedia.org/wiki/Autonomous_system_*(Internet)

(11) *https://www.redeszone.net/tutoriales/internet/que-son-root-name-server/*

(12) *https://en.wikipedia.org/wiki/Internet_exchange_point*

(13) *Cyber Key Terrain: A Conceptual Assessment*. US Naval Postgraduate School. Junio de 2016, *https://apps.dtic.mil/sti/pdfs/AD1111645.pdf* , todos consultados en julio de 2022.

soltura en todas las capas y situaciones del CE. Para diseñar e implementar una ciberfuerza eficaz y capaz es preciso especializar a los componentes de los equipos en áreas específicas.

Los equipos multidisciplinares requieren dominar aspectos sobre el espectro electromagnético; sobre tecnologías de operación (TO), sistemas de control (ICS, SCADA, PLC, IoT, vehículos autónomos, enjambres de drones, armas autónomas); sobre las tecnologías de información (TI); sobre inteligencia artificial, *big data*, realidad virtual; sobre redes sociales, ciberinteligencia, etcétera.

Las acciones en el ciberespacio tienen efectos en el mundo físico y en el cognitivo, y para saber lo que está pasando es necesario contar con una visión general que abarque a todos estos aspectos (*Cyber Situational Awareness*, CySA), visión de la situación que se obtiene merced a la ciberinteligencia.

Es, por tanto, necesario contar con estructuras, medios y personas para contrarrestar los efectos que el adversario quiera causar, en el ciberespacio y en los ciberlitorales, para perjudicar los intereses nacionales.

Como corolario, el imprescindible control centralizado de las ciberoperaciones no debe ser obstáculo para contar con cibercapacidades tácticas autónomas en apoyo de una operación convencional. Toda misión convencional tendrá sus aspectos CE, y el comandante debería contar con cibercapacidades orgánicas propias al nivel que se determine.

Por último, la existencia del CE y su estrecha relación con todas las tecnologías y con la información están llevando a integrar todas las capacidades relacionadas con la información (14) bajo un concepto unificador: *Information Warfare* (IW), que integra y coordina capacidades separadas como son *cyberwarfare*, EW, EMS, Intel, IO, Space o METOC.

(14) *https://en.wikipedia.org/wiki/U.S._Naval_Information_Forces,* consultado en julio de 2022.

Formación de aeronaves de la US Navy junto con *Harrier* de la Armada desfilando entre el USS *George H. W. Bush* y el *Juan Carlos I*. (Foto: Antonio Aparicio Méndez)