INFORMATION WARFARE, LA GUERRA DEL SIGLO XXI

Pablo MARTÍNEZ TRUCHAUD

La verdad es la primera víctima de la guerra.

Esquilo de Eleusis.

Introducción

L arte de la guerra se basa en el engaño», como afirmaba el general Sun Tzu en el primer capítulo de su libro *El arte de la guerra*, escrito hace más de 2.500 años en la antigua China. El engaño al que se refería este estratega consiste en el aprovechamiento de la información para generar una ventaja militar y, si fuera preciso, hacer uso de la desinformación para socavar la moral de un ejército enemigo o, todavía más importante, de su población, con el fin de que cese en su actitud beligerante o hasta que se consiga el objetivo perseguido.

La historia de los conflictos armados y de las relaciones internacionales han demostrado que, a través del engaño, afectando directamente a las percepciones, se pueden conseguir grandes victorias sin la necesidad de emplear la fuerza. Es la guerra de la información, o *information warfare*, un mundo extremadamente volátil y cambiante por la aparición de internet, pero tan antiguo como la guerra misma.

Además, es una forma de «combatir» extensamente empleada en conflictos que se mueven en la denominada zona gris, donde la principal ventaja, al igual que los ciberataques, es la difícil atribución o trazabilidad de esa desinformación.

Los conflictos de hoy, y con toda seguridad los del mañana, acompañarán sin duda, junto con el uso de medios militares, económicos y diplomáticos, a la explotación de la información. Estos medios, desarrollados bajo estricta coordinación y considerados tanto *hard-power* como *soft-power* en las relaciones internacionales, se proyectan sobre los ocho factores que definen el

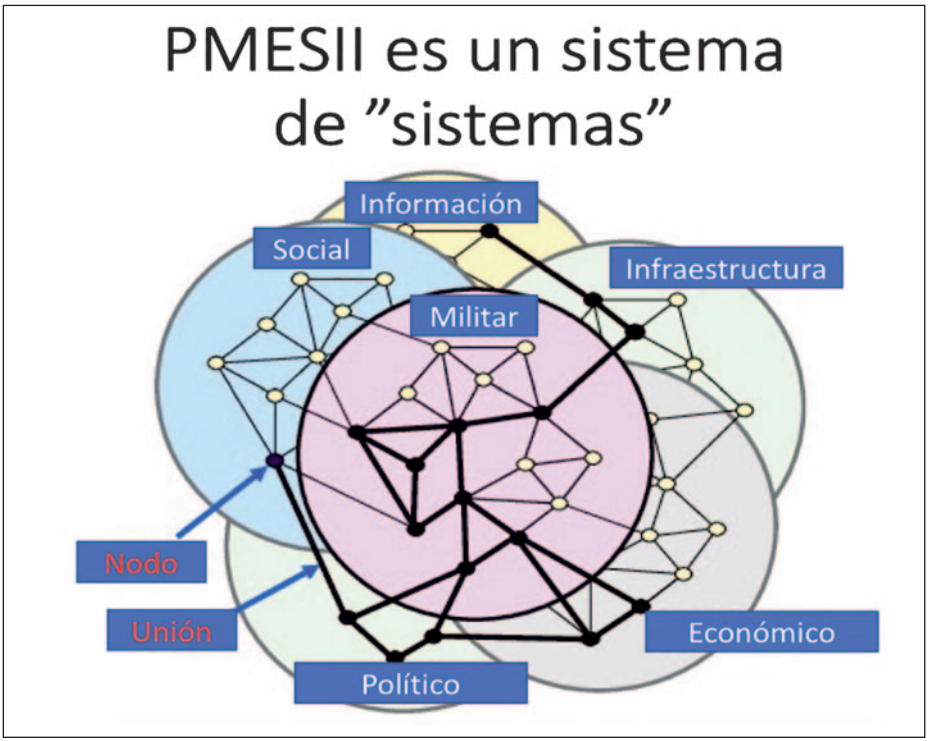
Segunda Guerra Mundial. Versión hinchable del carro de combate tipo *Sherman* del Ejército norteamericano, que se colocó masivamente en el estrecho de Dover, frente a la ciudad francesa de Calais, para hacer pensar a Hitler que el desembarco aliado en Europa sería en esa zona. (Fuente: Lorén, 2018)

entorno de cualquier actor estatal, el llamado entorno operacional o PMESII-PT (1), ampliamente utilizado en inteligencia. (EMAD, 2020).

La PDC-01 (A), *Doctrina para el empleo de las Fuerzas Armadas*, publicación doctrinal conjunta de más alto nivel en España, ya contempla un nuevo ámbito de las operaciones, el cognitivo, en el cual se hace incluso más importante la explotación de la información como ventaja militar y la concienciación de que perder esta primacía puede poner en peligro el transcurso de las operaciones y vidas humanas, tanto de fuerzas propias como civiles. Es un entorno que, junto al ciberespacial, es transversal a los ya conocidos marítimo, terrestre y aeroespacial. Es, en definitiva, un ámbito que afecta a las percepciones, y es ahí donde la información juega un papel fundamental.

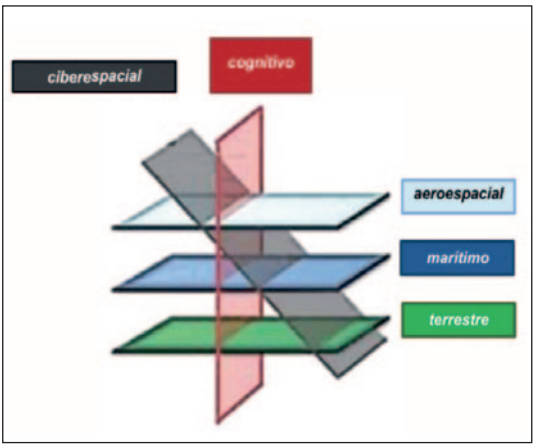
La *Estrategia de Seguridad Nacional de 2021*, recientemente publicada y que sustituye a la del 2017, incluye las campañas de desinformación como una amenaza que no había sido definida con anterioridad en su mapa de riesgos

(1) Político, Militar, Económico, Social, Informativo, de Infraestructuras, de Entorno Físico y de Tiempo.



Entorno PMESII-PT como un sistema de subsistemas. (Fuente: M. Ducote, 2021)

y que, citando este documento de alto valor estratégico-político, «tienen clara repercusión en la Seguridad Nacional y deben diferenciarse de otros factores como la información falsa —*fake news*— o información errónea —*misinformation*—». Además, otra novedad en este documento es que suscribe lo reseñado en la PDC-01 (A), considerando el ámbito cognitivo como un espacio más. (Presidencia del Gobierno, 2021).



Ámbitos de las operaciones. (Fuente: EMAD, 2018)

Precursoras de la *information warfare*, las operaciones de información

Para analizar globalmente el término *information warfare* es necesario hacer una retrospectiva hacia las operaciones de información, en adelante INFO OPS, fagocitadas técnicamente por esta guerra de la información.

Citando a la PDC-01 nuevamente, «las INFO OPS son la función cuya misión es coordinar las acciones de información para crear efectos deseados sobre los sistemas y procesos de información de los adversarios, reales o potenciales, y otras audiencias autorizadas, para influir en su voluntad, percepciones y capacidades, a la vez que se explotan y protegen los propios, en apoyo de la consecución de los objetivos operacionales y estratégicos» (EMAD, 2018).

Es decir, las INFO OPS son funciones de coordinación que promueven también percepciones y actitudes favorables a nuestros intereses y a su vez nos protegen de las de los adversarios.

Actualmente, las INFO OPS han pasado a ocupar una parte pequeña de todas las operaciones que abarcan las percepciones, pero lo que más las caracteriza es que la audiencia objetivo es principalmente el adversario, no la población en general o la opinión pública, siendo esta última una de las audiencias objetivo de la *information warfare*.

Dos soldados estadounidenses asistiendo a un soldado iraquí en el marco de la primera guerra del Golfo (1990-1991), también conocida como operación Tormenta del Desierto. Imágenes manipuladas deliberadamente para promover actitudes favorables o contrarias a Estados Unidos, tanto en Al Jazeera (izquierda), como en la CNN (derecha).
(Fuente: ArtOfficial Intelligence)

La OTAN, referencia doctrinal desde 1949

La Alianza Atlántica, en parte por las lecciones aprendidas de sucesos como la anexión ilegítima de Crimea por parte de Rusia en 2014, entre otros, se ha percatado de la extrema importancia de la *information warfare*. De hecho, recientemente, en enero de 2021, publicó el ATP-113 sobre *Maritime Information Warfare,* en adelante MIW, para definir todos los aspectos de esta «nueva» guerra que pueden afectar al planeamiento y conducción de las operaciones navales, especialmente a nivel táctico para un OTC (*officer in tactical command*) en la mar. De esta forma, la US Navy viene ejercitando esta figura a través de sus estados mayores desplegables en los grupos de combate de portaviones o *carrier strike groups*, con grandes núcleos de personal dedicados en exclusividad a este ámbito cognitivo.

La MIW queda definida como la actividad que emplea de forma segura, proporciona y protege la información, sus procesos, sistemas y redes, así como las actividades recíprocas para limitárselo, degradárselo y negárselo al adversario para alcanzar una ventaja operacional en el entorno marítimo.

Abarca todo tipo de actividades que engloban el ámbito cognitivo, desde la comunicación estratégica (STRATCOM), *public affairs* (PA), *military public affairs* (MilPA), diplomacia de defensa, *psychological operations* (PsyOps), INFO OPS, cooperación cívico-militar (CIMIC), guerra electrónica (EW), *key leader engagement* (KLE), *operational security* (OPSEC), cyber OPS*, military deception* (MilDec) y *navigation warfare* (NAVWAR). Son, por tanto, actividades que, si bien se desarrollan muchas de ellas en el nivel táctico, tienen un impacto enorme en el operacional e incluso en el estratégico, y conviene analizar previamente sus pros y sus contras haciendo una balanza de influencia *vs*. seguridad/OPSEC, es decir, influir sin revelar aspectos clave propios, denegando nuestros EEFI (*essential elements of friendly information*).

Al igual que la OTAN ha dado un paso adelante en la generación de doctrina táctica en el ámbito marítimo sobre *information warfare*, ¿no deberían a nivel conjunto desarrollarla también? ¿No es acaso una «guerra» que afecta a los cuatro ámbitos (ciberespacial, marítimo, terrestre y aeroespacial)? ¿Y no se debería a nivel conjunto nacional hacer lo propio? ¿Debe la Armada comenzar a conformar doctrina en este aspecto?

Las circunstancias internacionales actuales pueden dar respuesta a estas preguntas. Aparte del drama humanitario que está suponiendo la actual invasión de Ucrania por parte de Rusia, esta flagrante violación del Derecho Internacional consuetudinario le está sirviendo a Rusia para explotar al máximo sus capacidades propagandísticas y de *information warfare*, algo en lo que este país ya era un experto veterano.

Por tanto, la OTAN en su conjunto y España en particular, deben adaptarse y conocer perfectamente las tácticas, técnicas y procedimientos (TTP) de *information warfare* de potenciales adversarios para poder contrarrestarlas de

forma efectiva. Este efecto deseado, sin una generación doctrinal sólida y viva, puede llegar a ser inalcanzable.

Conclusiones

A pesar de la importancia de la *information warfare* en los conflictos del presente, especialmente en aquellos que se mueven en la zona gris, y siendo la información una de las denominadas funciones conjuntas —junto con otras como el mando y control, inteligencia, protección de la fuerza, etc.—, la doctrina sobre *information warfare* se encuentra poco desarrollada a nivel nacional conjunto. Cierto es que existe a nivel conceptual el ámbito cognitivo de las operaciones y que poco a poco se irá creando doctrina sobre ello conforme a lo estipulado en el documento *Objetivo de Doctrina a Largo Plazo (ODLP) 2035*, como ocurre por ejemplo con la «PDC 3.10. Operaciones de Información», actualmente en desarrollo, pero es preciso que ese incremento doctrinal vaya de la mano del avance tecnológico y del uso que se hace de él para influir en el potencial adversario, es decir, requiere proactividad.

No hay duda de que tal compenetración doctrinal necesita tiempo y múltiples debates y consensos, pero al ritmo que avanzan las operaciones en el ámbito de las percepciones se requiere una resiliencia si cabe mayor a la demandada a los ejércitos en general en el siglo XXI, el siglo de la «nueva» guerra.

BIBLIOGRAFÍA

EMAD (2018): *PDC-01 (A). Doctrina para el empleo de las FAS*. Ministerio de Defensa.

—(2020): *PDC-00. Glosario de terminología de uso conjunto*. Ministerio de Defensa.

—(2021). *Objetivo de Doctrina a Largo Plazo (ODLP) 2035*. Ministerio de Defensa.

—(2022). *Plan de campaña de desarrollo de doctrina, 2020-2025*. Ministerio de Defensa.

MONCADA LORÉN, Manuel (6 de junio de 2018): *National Geographic, https://www.nationalgeographic.es/historia/2018/06/el-desembarco-del-ejercito-fantasma-en-normandia*.

DUCOTE, Brian M. (2012): «Challenging the Application of PMESII-PT in a Complex Environment», *https://www.semanticscholar.org/paper/Challenging-the-Application-of-PMESII-PT-in-a-Ducote/32aa722aa90378caeaf589b425693f0d5e769c6e*.

TORRES-SORIANO, M. R. (2011): «Guerras YouTube. El impacto de las nuevas tecnologías de la información en el tratamiento mediático de los conflictos armados», *https://dialnet.unirioja.es/servlet/articulo?codigo=3838710*.

TORRES-SORIANO, M. R.; GARCÍA MARÍN, J. (2009): «Conflictos bélicos y gestión de la información: una revisión tras la guerra de Irak y Afganistán», *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-35692009000200002*.

Presidencia del Gobierno (2021): *Estrategia de Seguridad Nacional 2021. Un proyecto compartido. Gobierno de España*.