Temas de estrategia

Joint Force Quarterly (enero 2019)

Ficha	Sanchez, Frank; Lin, Weilun; y Korunka, Kent 2019 "Applying Irregular Warfare Principles to Cyber Warfare", *Joint Force Quarterly* 92 (enero) (Washington: National Defense University Press) pp. 15-22.
Autores	Commander Frank C. Sanchez, USN, is and Action Officer on the Joint Staff J32, Intelligence, Surveilance, and Reconnaissance Operations. Major Weilun Lin, USAF, is Chief of the Central and South Asia Branch, Joint Cyberspace Center, U.S. Central Command. Lieutenant Colonel Kent Korunka, USA, is a Joint Intelligence Planner, Joint Planning Support Element, Joint Enabling Capabilities Command, U.S. Transportation Command.
Palabras clave	Cyber warfare, irregular warfare, special operations, cyber operations, Cyberspace Diamond Model, cyberpower.
Tema	La aplicación de los conceptos y teorías de la guerra irregular a las operaciones del ciberespacio.
Argumento	El ciberespacio es un dominio de guerra relativamente nuevo que no se ajusta a las limitaciones físicas de la tierra, el mar, el aire o el espacio. A diferencia de estos dominios tradicionales, el ciberespacio implica la existencia de una amenaza impredecible que puede adaptarse, transformarse y reproducirse sin una identidad o rostro nacional. Es decir, no está restringido por los límites geográficos naturales y las reglas tradicionales de la guerra. Sin embargo, al integrar los principios de la guerra irregular con las operaciones del ciberespacio, se puede optimizar la asignación de recursos y mejorar la efectividad del poder cibernético. Las similitudes compartidas entre la guerra irregular y la guerra cibernética posibilitan el establecimiento de una base que guíe a los líderes de Estados Unidos en la ejecución de operaciones para mantener la superioridad cibernética. Al destacar cómo la guerra irregular y la guerra cibernética son similares, y al proporcionar el marco necesario para utilizar los principios de la guerra irregular para abordar, definir e integrar las operaciones del ciberespacio en todos los dominios y servicios, los dirigentes estadounidenses pueden aumentar la eficacia de la fuerza cibernética militar de Estados Unidos.
Descripción del mundo	El mundo es dinámico y los avances tecnológicos han generado que este espacio se consolide como un campo de guerra. Para enfrentar las amenazas que se desarrollan en este dominio es necesario aplicar estrategias de la guerra irregular.
Concepción de intereses estratégicos	Al comprender las similitudes entre las características, principios y teorías de las operaciones del ciberespacio y la guerra irregular, los líderes en los niveles estratégico, operativo y táctico podrán generar una teoría estructurada de la guerra cibernética para formular planes

	de ataque coherentes. Dicha teoría tendrá como objetivo conducir e influir en actividades, a través y desde el ciberespacio, para alcanzar los objetivos establecidos en la estrategia de seguridad nacional y buscará el control y la superioridad mediante la aplicación de las operaciones en el ciberespacio.
Concepción de guerra	La ciberguerra: los autores consideran que el ciberespacio presenta nuevas amenazas, ya que éste es un ámbito que no se ajusta a los límites físicos o convencionales de la guerra. De este modo, el ciberespacio fomenta una amenaza impredecible que puede ajustarse, transformarse y reproducirse sin una identidad o rostro nacional. Por tanto, la ciberguerra tiene el fin de ayudar a ganar el dominio político, económico, ideológico, social y religioso, y obtener información para transformarla en ventajas competitivas. Sus objetivos son elementos principalmente intangibles, como la información, y componentes tangibles, como los sistemas de información.
Concepción del enemigo o de las *amenazas*	Las operaciones del ciberespacio se caracterizan por estar expuestos a un entorno complejo –marcado por la inestabilidad y la ambigüedad- y por actos de violencia perpetrados por actores anónimos, ya sean individuos o personajes no estatales. > The new global domain of cyberspace relies on the connected information technology infrastructure that includes all the automation and networked system components through which information or content flows or is stored. Cyberspace operations are conducted in the physical network, logical network, and cyber-personal layers of the cyberspace domain. The ease of entry into cyberspace allows individual actors, criminal organizations, and small groups to operate in the cyberspace environment on a similar level as nation-states and transnational organizations. The anonymity and lack of attribution afforded actors in the cyberspace domain resemble the covert or clandestine aspects of [Special Operations Forces] SOF (Sanchez, Lin y Korunka, 2019: 17).
Fuerzas mencionadas en el artículo	U.S. Cyber Command Departamento de Defensa de Estados Unidos (DOD).
Metodología para *enfrentar* las amenazas	Los autores realizan una tabla comparativa en la cual se puede observar que la guerra cibernética y la irregular cuentan con varias similitudes, entre las que se pueden destacar los propósitos y la estrategia. Los objetivos de ambas guerras son ayudar a obtener el dominio político, económico, ideológico, social y religioso, y conseguir información para adquirir ventajas competitivas. Por otro lado, la estrategia se basa en el uso de operaciones directas y/o encubiertas, y en las atribuciones de inteligencia. A partir de lo anterior, los autores señalan que la forma de constituir una teoría del ciberespacio debe hacerse a través de la inclusión de conceptos, métodos y tácticas de la guerra irregular, ya que ésta utiliza actores que se adaptan fácilmente a las condiciones complejas del entorno. Así, conceptos como superioridad relativa y ciberpoder toman relevancia, definiéndolos de la siguiente manera:

	At the strategic level, cyber power is the combined strength of a nation's cyberspace capabilities to conduct and influence activities in, through, and form cyberspace to achieve national security objectives in peacetime and across the full spectrum of conflict. At the operational and tactical level, it is also the control and relative superiority gained by application of cyberspace operations over an adversary that uses technology as a means to contest integrity, confidentiality, security, and accessibility of information (Sanchez, Lin y Korunka, 2019: 19). Se retoma un marco de referencia de la guerra irregular titulado "Counterinsurgency Diamond Model" de Gordon McCormick para constituir un modelo para las operaciones del ciberespacio denominado "Cyberspace Diamond Model", el cual promueve la legitimidad de la información en el ciberespacio a través de la buena gobernanza, una mayor seguridad y transparencia. El modelo está conformado por cuatro elementos: 1. Población: los usuarios del ciberespacio, pueden ser humanos o máquinas. 2. Disruptores: son humanos, máquinas, gobiernos y/o criminales que realizan o apoyan operaciones para interrumpir o alterar la disponibilidad, seguridad, confidencialidad o integridad de la información del ciberespacio. 3. Controladores: son las fuerzas administrativas de una sección del ciberespacio. Pueden ser administradores de redes o gobiernos nacionales. 4. Gobernanza: son las estructuras y procesos diseñados para garantizar la rendición de cuentas, la transparencia, la capacidad de respuesta, el estado de derecho, la estabilidad y una participación amplia. Incluye a Estados externos, organizaciones internacionales y otros grupos que no apoyan el papel de los controladores y disruptores. Los controladores y disruptores deben realizar operaciones tomando en consideración la retroalimentación o *feedback,* así como la manera en que la población y la gobernanza percibirán la legitimidad de su información. Para ello, los autores destacan el uso de cinco estrategias a lo largo del conflicto del ciberespacio. 1. Apoyo de la población: el objetivo es obtener el apoyo de la fuente de poder, es decir, la población. 2. Disrupción de la información: se busca prevenir o interrumpir el control de la población por parte del oponente, esto es, a través de la creación de una brecha entre los disruptores y la población al deslegitimar la información generada por los primeros. 3. Acción directa: está dirigida a atacar al oponente para

	romper con sus operaciones y negar su habilidad para continuar en el conflicto. 4. Interacción disruptiva: ambas fuerzas necesitan legitimad para obtener el apoyo y el acceso a la gobernanza. Para lograrlo, los controladores deben atacar la legitimidad de la información de los disruptores, mientras mejora su relación y confianza con la gobernanza. Relación con la gobernanza: establece que, a nivel del Estado-nación, la gobernanza y el apoyo internacional pueden brindar legitimidad a la información de los controladores.
Documentos militares citados	Joint Publication (JP) 3-05, *Special Operations.* Joint Publication 3-12 (R), *Cyberspace Operations.* *Joint Operating Environment (JOE 2035): The Joint Force in a Contested and Disordered World.* *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command.* Air Force Doctrine Document (AFDD) 3-12, *Cyber Operations.* Joint Publication 5-0, *Joint Planning.* Department of Defense, *Department of Defense Strategy for Operating in Cyberspace.*
¿Cómo se inscribe esta discusión en el tema de nuestro proyecto?	La incorporación de elementos de la guerra irregular a una nueva concepción de la guerra en términos del ciberespacio, permite entender cómo es que Estados Unidos está definiendo y caracterizando la guerra y las amenazas actuales para así generar estrategias que fomenten la superioridad cibernética.
Enlace electrónico del artículo original	https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1737001/applying-irregular-warfare-principles-to-cyber-warfare/
Persona que elaboró la ficha	Ana Katia Rodríguez Pérez