Temas de tecnología

Military Review (septiembre-octubre 2019)

Ficha	Orinx, K. Struye de Swielande, T 2019 "A Chinese Fox against an American Hedgehog in Cyberspace", *Military Review* (septiembre-octubre) (Washington: National Defense University Press) pp. 58-66.
Autor	*Kimberly Orinx* is a PhD candidate and teaching assistant at Université Catholique de Louvain, Belgium. Her research focuses on cyberspace and the China-Russia-United States triangle. She holds an LLM in international law from the Free University of Brussels and two master's degrees in international relations from Tongji University (Shanghai, China) and the Free University of Brussels. *Tanguy Struye de Swielande*, PhD, is a professor of international relations at Université Catholique de Louvain, Belgium. He is the founder of the Genesys Network and the director of the Center for the Study of Crisis and International Conflicts. He is also a research fellow at the Egmont Institute and guest lecturer at the Belgian Royal Military Academy.
Tema	La implementación de estrategias integrales para superar la pérdida de poder discursivo y narrativo de Estados Unidos en el ciberespacio como elemento fundamental para el mantenimiento de la hegemonía.
Argumento	El régimen de Donald Trump ha invertido en una lógica de poder duro, lo cual es útil para influir en el corto plazo. Sin embargo, para tener injerencia a largo plazo y mantener la hegemonía es indispensable utilizar otras herramientas de poder, ligadas al consenso -como la sociabilidad y la persuasión-, las cuales se pueden implementar de manera eficiente en el ciberespacio.
Palabras clave	Cyber warfare, cyber sovereignty, reverse censorship
Descripción del mundo	El mundo es complejo. En este medio, la digitalización y la información fungen como elementos indispensables para el mantenimiento de la hegemonía.
Concepción de guerra	La guerra está vinculada con la capacidad de consenso de los actores a nivel internacional. En este contexto, el ciberespacio es fundamental, ya que este medio no sólo permite atacar infraestructura clave, sino que también pone en riesgo el sistema político y los valores de occidente.

	> As stressed by the Russians, the main battlefield is human consciousness, perceptions, and strategic calculations (p. 59). Así, la guerra no solo incluye elementos militares o políticos, sino también sociales, en donde la información es un factor fundamental para el éxito.
Concepción del enemigo o de las *amenazas* (threats)	Estados Unidos considera que tanto Rusia como China son Estados revisionistas que compiten en el escenario clásico (económico y militar), pero también en el discursivo e ideológico. China está desarrollando una estrategia más integral en el ciberespacio, por lo que es la principal amenaza para la hegemonía estadounidense, sobre todo en el ámbito del consenso. Las amenazas en el ciberespacio implican la influencia que otros Estados puedan tener sobre la población del territorio implicado y esto se vincula con la ciber-soberanía. > The concept of cyber sovereignty is based on two main principles: (1) banning unwanted influence in a country's "information space," and (2) shifting the internet governance from current bodies that include academics and the private sector to an international forum such as the United Nations that would imply a transfer of power to states alone (p. 61). Tanto China como Rusia prefieren usar el término "information security" en lugar de ciber-soberanía, debido a que este incluye las dimensiones técnicas y cognitivas de los ciberataques. Otra amenaza identificada por los autores y vinculada con la ciber-soberanía es "reverse censorship", que se vincula con la manipulación que puede haber en las poblaciones a través de las redes sociales. Esta es una de las principales amenazas para el gobierno estadounidense, sobre todo considerando la cantidad de horas que las y los estadounidenses ocupan navegando en la web. La RAND denomina a esta acción "influence operations", la cual > encompass activities undertaken in cyberspace affecting the cognitive layer of cyberspace with the intention of influencing attitudes, behaviors, or decisions of target audiences (p. 63).
Metodología para *enfrentar* las amenazas	Delinear el ambiente de los adversarios (limitar su capacidad de movimiento, sus opciones, posibilidades y proyecciones) a través del ciberespacio para fomentar su declive y garantizar la supremacía estadounidense. La estrategia utilizada por Trump debe ser modificada. Se sugiere la creación de un nuevo excepcionalismo estadounidense, con una estrategia narrativa diferente que garantice que Estados Unidos mantenga el orden internacional que le convenga.

	> This art of influence, the interconnected nature of information, and the characteristics of cyberspace blurred the lines between war and peace with actions beyond normal peacetime competition but short of all-out war and made the clear distinctions between military and civilian almost impossible. This gray zone, where the tools employed will remain short of high intensity, creates an interval in which strategic narratives and other influence tactics play a key role (p. 64). Asimismo, el internet debe ser considerado el campo de batalla donde se disputa la hegemonía.
Documentos militares citados	The National Security Strategy of the United States of America Tallinn Manual (a study on international law's application in cyber conflict and cyber warfare) 2010 Information Office of the State Council's "White Paper on the Internet in China" De China: The 2015 Ministry of National Defence of the People's Republic of China's paper "China's Military Strategy" 2013 Science of Military Strategy 2012 PLA's glossary of military terms Communique on the Current State of the Ideological Sphere 2015 National Security Law of the People's Republic of China
Comentarios	De acuerdo con el sistema de Martin Libicki, el ciberespacio está formado por tres capas: > The physical layer (the hardware—tangible objects like computers, servers, routers, etc.), the syntactic or logi-cal layer (software, protocols, etc.), and the semantic or cognitive layer (information and ideas) (p. 60). Los primeros ataques cibernéticos se enfocaron en dañar infraestructura, no tanto en manipular los valores e ideas de las y los demás. > The first events that come to mind when considering cyberattacks are the Estonian cyberattacks (2007), the Stuxnet virus (2010), and the WannaCry software (2017), which were all attacks on infrastructure (p. 59).
¿Cómo se inscribe esta discusión en el tema de nuestro proyecto?	Gramsci mencionaba que la hegemonía se articula a partir de la coerción y el consenso. En ese sentido, debido a la asimetría de poder que existe entre los sujetos que se disputan la hegemonía, otros espacios se han consolidado como estratégicos para el mantenimiento de la hegemonía y el consenso es una herramienta central para la conservación o el establecimiento de un orden global particular.

Enlace electrónico	https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/SO-19/Struye-Orinx-Fox-Hedgehog.pdf
Persona que elaboró la ficha	Adriana Franco Silva