TEMAS DE ESTRATEGIA

Revista Military Review (Septiembre-Octubre 2020)

Ficha	Tosi, Scott, Capitan U.S Army, 2020 "Steal The Firewood from Under he Pot: The role of intellectual property Theft in Chinese Global strategy", *Military Review*, Septiembre – Octubre 2020, Kansas: Army University Press) pp. 95 - 109.
Autor	Capt. Scott Tosi, U.S. Army, is the company commander for Headquarters and Headquarters Company, 501st Military Intelligence Brigade in Camp Humphreys, Korea. He holds a BS in history and social sciences education from Illinois State University and an MPA from the University of Illinois–Springfield. His assignments include Yongsan, Korea; Fort George G. Meade, Maryland; and Camp Lemonnier, Djibouti.
Palabras clave	Propiedad Intelectual, Ciberguerra, Seguridad de la información.
Tema	La importancia de la protección de información en el desarrollo de tecnología estratégica.
Descripción del mundo	Un mundo en el que China contiende de manera explícita con Estados Unidos por el estatus de superpotencia. Se hace alusión a que esa disputa por la hegemonía se lleva a cabo por medios ilegítimos, como el robo de propiedad intelectual.
Concepción de intereses estratégicos	Desde la perspectiva China, estos consisten en proveerse de seguridad y competitividad (militar y económica) por medio de independencia y superioridad en tecnología. Desde la perspectiva estadounidense, la protección de información le otorga una ventaja competitiva en lo militar y económico.
Concepción de guerra	Comprende tanto la de corte tradicional, como la económica, jurídica, cibernética y tecnológica.
Concepción del enemigo o de las amenazas (threats)	El enemigo de Estados Unidos es China por estar explícitamente resuelto a contender y competir en las esferas económica y militar para ascender como potencia hegemónica. Para ello se lleva a cabo una estimación sobre los alcances del robo de propiedad intelectual: > According to a 2013 report by Verizon, 96 percent of all cyber espionage data breach cases were attributed to threat actors in China. China utilizes state, business, and private cyber actors to compromise and steal $180 billion to $540 billion of IP and trade secrets annually, or 1 to 3 percent of the U.S. GDP. "These cyber-enabled campaigns threaten to erode U.S. military advantages and imperil the infrastructure and prosperity on which those advantages rely." (Tosi 2020: 105).

Fuerzas implicadas en el artículo	US Army, DOD.
Metodología para enfrentar las amenazas	Fortalecer las medidas de protección de datos del DOD expandiéndolas a instituciones y agencias con las que colaboran: > To mitigate and prevent IP theft, the DOD must strengthen existing government, private, and academic partnerships, committees, and policies. (Tosi 2020: 106) Expandir la cobertura de medidas de protección de información tecnológica más allá de la etapa de desarrollo: > Furthermore, the DOD and other government agencies must ensure protection of technologies from "cradle-to-grave," a term used to describe protection of critical technologies from the time of their inception through their fielding, lifecycle, and eventual replacement by new technology. (Tosi 2020: 106).
Mecanismos o planos de la guerra contra el enemigo o las amenazas	La amenaza y guerra se desarrolla en el plano económico, cibernético y social, en universidades, empresas, institutos de tecnología y gobiernos y por medio de políticas. El artículo tiene un enfoque defensivo más que de ataque ante las amenazas. La guerra se desarrolla en el plano de políticas gubernamentales para la mitigación de la amenaza, en el plano legal e institucional.
Documentos militares citados	• The White House, National Security Strategy of the United States of America (Washington, DC: The White House, 2017), 21, accessed 14 May 2020, • Field Manual 3-0, Operations (Washington, DC: U.S. Government Publishing Office, 2017), 1-1–1-2, • Select Comm. on U.S National Security and Military/Commercial Concerns with the People's Republic of China, H. Rep. No. 105-851, at x–xi (1999), accessed 14 May 2020, • "Contracts," DOD, accessed 15 May 2020, • Senate Comm. on Armed Services, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, S. Rep. No. 112-167, at vi–viii (2012), accessed 15 May 2020, • Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019 (Washington, DC: DOD, 2019), 65, accessed 18 May 2020, • DOD 5220.22-M, *National Industrial Security Program Operating Manual* (Washington, DC: DOD, 2006, incorporating change 2, 18 May 2016), accessed 18 May 2020, • "DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)," Office of the Under Secretary of Defense for Acquisition, 31 December 2019, 252.204-7012(m)(2), accessed 10 March 2020,

	• "DFARS 252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services (Dec 2019)," Office of the Under Secretary of Defense for Acquisition, 31 December 2019, 252.204-7018, accessed 18 May 2020.
¿Cómo se inscribe esta discusión en el tema de nuestro proyecto?	Siendo un escenario muy relevante de la competencia de grandes potencias, la propiedad intelectual es el mecanismo de preservación de la ventaja adquirida a través del desarrollo de tecnología en los planos comercial, económico y militar.
Enlace electrónico al artículo original	https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2020/Tosi-Intellectual-Property-Theft/
Persona que elaboró la ficha	Programa de servicio social "América Latina en la Geopolítica Mundial."