What Is a Cyber Warrior? The Emergence of U.S. Military Cyber Expertise, 1967–2018

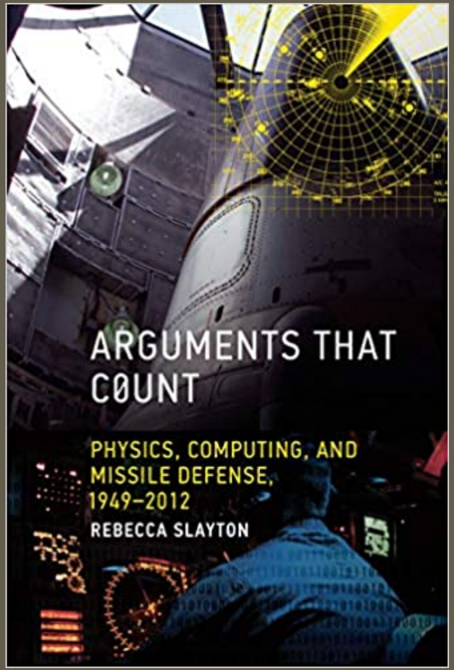
April 30 12 pm

https://umsystem.zoom.us/j/93549664745

With Rebecca Slayton, Associate Professor, Department of Science and Technology Studies, Cornell University

Slayton's research and teaching examine the relationships between and among risk, governance, and expertise, with a focus on international security and cooperation since World War II.

How have military cyber operations, a diverse set of activities that often differ little from civilian cyber security work, achieved the status of "warfighting"? What activities have the greatest warfighting status, what activities have the least, and why? This paper examines the establishment and growth of expertise associated with cyber operations in the individual services and at the joint level since the late 1960s. Threat-oriented activities, such as attacking adversaries or responding to adversaries that have breached U.S. networks, have more readily achieved warfighting status than have vulnerability-oriented activities, such as patching software, training users in good security practices, and other actions that aim to prevent intrusions. Ultimately, the lower status of work and expertise associated with vulnerability mitigation remains a significant problem for military cyber operations.



Link to the article version of the talk:
https://tnsr.org/2021/01/what-is-a-cyber-warrior-the-emergence-of-u-s-military-cyber-expertise-1967-2018/

Sponsored by the Center for Science, Technology, and Society
https://csts.mst.edu/