2d Lt James Marvin

CTC #3

To grasp cyber in a military context you must think of it as a domain. This is in accordance with the National Defense Strategy of the United States for 2018 1. In warfare the domain is where the actions of the conflict are taking place. Lieutenant Colonel Bryant’s paper examines domains using a dichotomous model of ways and means 2. He provides an example model using the air domain. The ways in this case are the fighters, bombers, UAVs, etc. and the means are strategic attack, ISR, Logistic Support, etc. Bryant is quick to point out that cyber has its own unique characteristics that affect defining its domain. The first is that the geography of cyber is mutable due to its artificial nature 2. The second unique characteristic is how cyber effects can bleed over into the other domains. He provides an example of inserting misleading logistics information to position ground forces in an advantageous state for enemy forces 2. Third, there is an inherent asymmetry between offensive operations and defensive operations 2. The cost to penetrate a network is pennies on the dollar compared to defending one. Despite these unique circumstance Bryant can provide a ways and means model for the cyber domain. The means include tools such as social engineering, denial of service, and SCADA attacks. The means include effects such as information war, intelligence collection, and reduction of enemy logistics 2. This model works best in describing cyber as the arena for cyber conflict but fails to recognize how this domain is present in the operations of all service components. Our military is organized into components based on the traditional domains of previous combat: air, land, and naval. The problem is cyber is a military wide domain, but we restrict much of the operations to a single branch, Air Force. It is probably safe to conclude that cyber is a domain that encompasses other domains which is not possible in the traditional definition of a domain. For example, the land domain does not encompass the sea domain. Despite this, I still believe that looking at cyber as a domain where we conduct military operations to be a correct warfighting analogy to describe the reality of the situation.

Sources:

1. Mattis, Jim. "Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military’s Competitive Edge (Washington DC: US Department of Defense, 2018)." 3-27.
2. Bryant, William D. *Cyberspace superiority: a conceptual model*. AIR UNIV MAXWELL AFB AL AIR FORCE RESEARCH INST, 2013.