

The article "Social Cybersecurity: An Emerging National Security Requirement" by Lt. Col. David Beskow and Dr. Kathleen Carley explores the importance and scope of social cybersecurity as a crucial component of national defense. Information strengthens a nation as a power. Rather than depending on digital infrastructure, they explore the avenues of social cybersecurity by manipulating information and social structures. For example, Russian information operations utilize "active measures" to sow division within societies, often leveraging local social media platforms. This is a strategic attempt to destabilize a nation without traditional warfare. The article introduces the BEND model (Back, Engage, Neutralize, Dismiss) to categorize tactics for manipulating information to amplify divisive content. Techniques like "thread jacking" and "community bridging" demonstrate the sophistication with which adversaries can subtly infiltrate and manipulate social networks to influence opinions. The authors emphasize the need for military leaders to recognize the threat vector and understand social cybersecurity is essential for national security. Particularly as misinformation becomes a potent tool in national power dynamics. For the U.S. Department of Defense, this requires policies that allow for agile responses in the information domain while educating the public on recognizing and mitigating misinformation.