In this journal I will summarize my response to the article: social cybersecurity an emerging national security requirement (Military review, 2019). The article identifies social cybersecurity as a new front in the field of asymmetric warfare. With technology enabling both peer competitors and non-state actors to manipulate the public square of discourse not only nationally, but globally as well. The ideas behind information warfare are nothing new, whether the propaganda used by all sides during World War II, the idea of hearts and minds pushed during the Vietnam war or controlling the narrative of today's news cycle and social media. It's all based in controlling the flow and shape of information, the multidisciplinary scientific tools and techniques and technology brought to bear have merely evolved. Coupled with the ubiquitousness of our global digital space is what gives this new facet of asymmetric warfare its ability to act as a force multiplier.

The core goals of offensive use of social cybersecurity to is disrupt, distort, and divide. To weaken trust in national institutions and consensus and commitment to traditionally shared values through misinformation, manipulation, or distortion of information. The idea of using bots as force multipliers is something read about before, but while the core goals resemble some of the traditional information warfare tactics I've seen in the military. The forms of social-cyber maneuver: thread jacking, smoke screening and hashtag latching, Opinion leader co-opting, community bridging and false generalization are all tactics in information and network maneuver is something I have no experience with. What I do find interesting, is what the article doesn't talk about. That's the ease by which peer competitors and non-state actors gain access to staggeringly large amounts of data with which to conduct these operations. It's notable that the article doesn't address the largely unregulated mass collection of information, clearly private and often without consent that helps feed these malicious actors and their operations. Another facet that should be explored are the effects of unregulated data brokers and tech companies commodifying personal data and selling it to entities that are very clearly hostile to not only the United States but to the EU as well.

References

Social Cybersecurity an emerging national security requirement. Army University Press. (n.d.). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/