2d Lt Marvin

Paper Abstract

The Air Force mission reinforces the notion that winning in cyberspace is a necessity. The Air Force could be more successful at winning in the cyber domain if they could devote more manpower to the offensive operations in cyber. The Air Force has been bogged down trying to handle the seemingly infinite number of incoming threats that they have been struggled to prosecute the actors creating the threats. The easy solution would be to simply bring in more people, but history has shown that there is a lot of competition for security professionals because cyber touches all facets of the economy. The solution that this document proposes is that the Air Force shift a sizeable portion of Airmen from its defensive and maintenance operations to the pointy tip of the spear. The shift will be able to take place through the help of network defense tools coupled with machine learning that will alleviate the number of actions performed by network defenders and maintainers.

The value of this paper will be to provide the decision makers in manpower a clear direction for how to make this transition happen. Much of the evidence for the proposed plan will come from case studies of very similar transitions happening in various industries. Most corporations have a miniscule bandwidth for cyber operations compared to the Air Force. This has forced them to lean into solutions that use automated network defense because they often lack even a few people to handle the thousands of network events daily. The intended result of this paper is to extrapolate how to apply these solutions to the complex landscape of Air Force cyberspace operations.