This article painted a picture of the struggle the DOD is currently going through to provide the manpower necessary to meet the operational challenges of the cyber domain. This year they elevated CYBERCOM to a full combatant command level made up of 133 teams and 6200 people. This elevation does not signify that the command has reached all its goals. Quite the contrary, each service is hard pressed to find individuals that can make it through the NSA’s RIOT course that is required to be an operator using their cyberwarfare infrastructure. Each service has resorted to implementing lower level training courses so that the barrier to entry into the cyber mission teams is lower. Only the “star athletes” of these lower level training course get to attend RIOT.

The two main problems are recruiting and retention. This article succinctly put that the challenge to recruiting is that there is an overwhelming demand for security professionals both within and outside the military. The organizations outside the military can often provide greater financial benefits and a “much less maddening bureaucracy”. And retention is tricky because it takes over two years to train most military cyber operators and that is almost halfway done with their commitments so the amount of use we get might only be a few years before they are drawn to work somewhere else. I believe the key is providing the right incentives to cyber operators that make staying a completive offer. Another route proposed by General Crall was to find new ways of getting military members with no formal in cyber opportunities to try it out. There are plenty of servicemembers eager to get experience in this valuable field.