Opinion

Warrant officers should be the next cyber operators

By **Jeremiah Pittman** and **Jan Kallberg**

Apr 20, 2020

Georgia Army National Guard Capt. George Allen, a network engineer, takes the drivers seat for Team National Guard during the U.S. Army's 'Cyber Center of Excellence', Fort Gordon, Ga. (Staff Sgt. Tracy J. Smith / Georgia Army National Guard)

Our proposal is straight forward.

There is too much turnover among non-commissioned officer (NCO)/enlisted cyber operators to match the expanding need for a highly qualified and technically cognizant cyber force. But there are lessons to be learned from

other military career fields, which there is a high educational and technical investment upfront (Think of Army aviation or the medical field.) We propose that the cyber force, instead of relying on NCO/enlisted operators, replace these positions with warrant officers with a longer initial time commitment, higher return on the initial investment, and the potential for consolidating organizational knowledge in a more mission effective way.

We propose that there should be an option for immediate entry into the cyber operator WO track. Relied on as technical experts, WOs usually are drawn from the midgrade and senior NCO ranks. In the same way as in aviation, not everyone will have the whole kit to be successful, but for those who have what it takes, the Army would benefit from a six-year commitment instead of a three-year commitment. The proposed model mimics the Army aviation model of "street to seat," where able high school graduates can pursue an Army aviation career without any prior military service and go directly to Warrant Officer Flight School. This model would also enable stricter tailoring of what skillsets the force wants at the point of entry, and it offers enough time to modify and upgrade skillsets. It allows more freedom for talent management incentives. The cyber operators of the 2020s and beyond will face increased technical complexity, accelerated decision cycles, and shorter time frames to grasp what's happening. In our view, that does not lend itself to enlisted/NCOs that are rapidly cycled through the system.

Why is this an issue – and what are we trying to solve?

The return on investment to train enlisted personnel to become cyber operators could be improved. The retention of cyber NCO who are operators is too low, as many seek opportunities outside of DOD directly after their first contractual obligation of three years. If it takes 15 months to train an enlisted cyber operator, including basic training from enlistment, and they phase out under their last three months, that means for half of their three-year tenure, they are not a contributing part of the cyber force. If we add other disruptions such as organization changes, retraining, and change of duty station, the actual productive time might be even far less.

Cyber is fast-moving and ever-changing, which requires a technical expert with longevity. Threat intelligence and the ability to understand the modus operandi of an adversary require experience. The adversary, even if supported by automated processes, is governed by human minds, with preferred tactics and techniques, which lend themselves to early identification and interception. These skills require, in a best case scenario, more exposure to the cyber operational environment than slightly more than a year. The argument against this is that operators should not make decisions. That argument fails, because if the operator is not able to identify and assess what is happening, then there is no relevant feedback loop to any leader. The whole mission team is stuck in a fog of war, filled with confusion and illusion.

Understandably, NCO/enlisted cyber operators seek to leave the Army for higher-paying jobs in the civilian job market after their three-year obligation to serve. The all-volunteer force provides that option. Future cyber operators will face a different civilian cybersecurity job market with increasing competition from cybersecurity majors from universities and IT-professionals that have retailored their careers, which increases the supply of cybersecurity professionals.

Our increased longevity might provide future veterans a 30 to a 50-year civilian career. The cyber WO leaving after six years would then be better positioned for a more competitive job market, ensuring higher lifelong earnings, and having a significant advantage over those who leave the Army after three years as well as civilian graduates. The change from enlisted/NCO cyber operators to WO cyber operators is a win-win, for the contracted individual, the mission, and the Army.

CW3 Jeremiah Pittman is a research scientist focusing on electronic warfare at the Army Cyber Institute at West Point and previously served in the 75th Ranger Regiment. Jan Kallberg, Ph.D., is a research scientist at the Army Cyber Institute at West Point, the managing editor for the Cyber Defense Review, and an assistant professor at the U.S. Military Academy. The views expressed are those of the authors and do not reflect the official policy or position of the Army Cyber Institute at West Point, the U.S. Military Academy, or the Department of Defense.